INFORMATION *and* INFORMATION TECHNOLOGY ASSURANCE

for IT managers

First Edition

David C. Chan

INFORMATION AND INFORMATION TECHNOLOGY ASSURANCE *for IT Managers*

First Edition

Additional copies may be purchased from:
York University Bookstore
4700 Keele Street
Toronto, Ontario
Canada M3J 1P3
www.bookstore.yorku.ca

Printed by York University Bookstore
Printed in Canada

INFORMATION AND INFORMATION TECHNOLOGY ASSURANCE

Preface

No one would doubt that information and information technology (I & IT) are playing an increasing role in business operations and our daily lives. The main reason for using computers is to be more efficient. This allows organizations to be more competitive. It also enables individuals to have higher earning power and achieve a better quality of life. Increasingly, organizations are finding it necessary to use technology in order to compete, and survive.

There are risks in using technology. It might be incorrectly applied because of inadequate training or unrealistic expectation on what can be achieved. Computer systems reduce paper and visible audit trail so errors have a higher chance of remaining undetected. There is higher concentration of processing when computers are used and this increases the impact of incorrect functions. Access to computer systems is less noticeable than access to paper files so the risk of unauthorized transactions can increase.

The purpose of this book is to help understand how I & IT affects risks, what internal controls should be implemented to mitigate risks and how internal controls can be tested and assessed to provide assurance to management and customers and auditors.

Information technology (IT) is a collection of computer resources, including hardware and software, used to process data and produce useful information. In this book, we will address the risk and control implications of information and information technology. We stress both because information sometimes may not be part of technology implementation but still needs to be controlled.

Resources for this book, including URLs, are referenced throughout the text as much as practical. I have made every attempt to acknowledge sources, although most of the material comes from my own experience and research. In a volume of this size, it is inevitable to have some errors or omissions, including acknowledgements. I ask that any reader who notices such omission contact me directly.

David C. Chan, MS, CPA, CISA, CISM, CISSP, CIA, CFE, PMP
June, 2015
York University

INFORMATION AND INFORMATION TECHNOLOGY ASSURANCE

About the author

David C. Chan is a highly experienced IT security and audit professional who has extensive experience in public accounting, banking and the public sector. He has many years of IT audit and security management experience in PwC, Bank of Montreal, Office of the Auditor General of Ontario, Hydro One and Ontario Treasury Board Secretariat. David has taught information systems auditing in Ontario universities. In addition to his degree of Master of Science in computer science, David has earned the following professional designations:

- Chartered Professional Accountant
- Certified Information Systems Auditor
- Certified Information Security Manager
- Certified Information Systems Security Professional
- Certified Internal Auditor
- Certified Fraud Examiner
- Project Management Professional

David has been active in professional research with Chartered Professional Accountants Canada (CPA Canada), Chartered Professional Accountants Ontario (CPA Ontario) as well as Information Systems Audit and Control Association (ISACA). He has served on the CPA Canada IT Advisory Committee, the CPA Ontario Course Content Committee and the ISACA Test Enhancement Committee. David has published in CPA Magazine and Information Systems Control Journal on the topics of audit risk and cryptography. David has also taught the preparatory courses for the CPA Ontario Core Knowledge Examination and the Certified Information Systems Auditor Examination.

Table of Content

Table of content

Table of content

Computer crime has increased in volume, impact and variety in the last two decades mainly because of the Internet. There are broadly speaking, two types of computer crime: crime causing fairly immediate damage like hacking, and crime that is fraudulent in nature like an email scam. In either case, the crime may be committed on IT resources or it may use IT as a tool to achieve the criminal intent. We will cover the following topics.

- Common computer crimes
- Common computer frauds
- Controls against computer crime and computer fraud
- Computer forensic investigation

CHAPTER ONE – WHO, WHAT, WHEN, WHERE, WHY?

Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other. – Bill Gates

There are risks in using information technology (IT). It might be incorrectly applied because of inadequate training or unrealistic expectation on what can be achieved. Computer systems reduce paper and visible audit trail so errors have a higher chance of remaining undetected. There is higher concentration of processing when computers are used and this increases the impact of incorrect functions. Access to computer systems is less noticeable than access to paper files so the risk of unauthorized transactions can increase.

Users of information and information technology (I &IT) need assurance in order to have faith in what they rely on to perform business transactions and make decisions. They want to have faith in the information to be provided by the organizations they work in or deal with. They have a right to demand that such faith be supported by a rigorous process of system assurance.

Some have said that computing power doubles every year, i.e., the IT capability costing a dollar today will probably cost fifty cents in a year. We have seen many examples of this in personal computers, storage devices and consumer electronics. This does not mean that consumers and organizations will spend less on IT. What this means is that we can continuously upgrade the use of IT to improve efficiency as well as information reach and richness, which can lead to better quality of life and more wealth. For organizations, this will increase competitiveness. To respond to demand, and to generate demand, technology product developers will continue to come up with new gadgets, tools and applications.

The speed of change in IT and the seemingly exponential adoption rate by users and organizations sometimes generate a question in one's mind about reliability. This is analogous to the doubt on quality and safety that rises from increasing the speed of driving or high staff turnover. How is reliability measured? Who will measure it? Who will assure it? With increasing use of the Internet, these questions will be asked more often, and by more people. The Internet has changed the world and will continue to change it.

In 1998, Reza Raji, a senior engineer in IBM, asked in an Institute of Electrical and Electronic Engineers forum, "What if the Internet was allowed to go beyond connecting desktops and laptops and could somehow be tied to the devices around us?" He further illustrated the connectivity mechanism as a natural extension of "the networking paradigm into control devices by allowing the different networks to join and form a homogenous networking fabric. In the same way that the intranets became an extension of the Internet, the local operating control networks, …could be linked to the Internet and

intranets where information (data and control) could flow from anywhere to anywhere, from anybody to anything. People could now reach things as well as other people." The Internet is growing in this direction. It is called the Internet of Things (IoT).

In IoT, all types of network-connected devices and appliances are fitted with sensors that send and receive data. For example, a refrigerator can tell its owners when they are low on mustard, or a thermostat can adjust itself based on whether it senses human presence in a room. The Google Glass and Apple's iWatch are delivering similar functions. . While predictions vary depending on which report you read, Gartner, Inc. estimates that IoT will include 26 billion units installed by 2020, and by that time, IoT product and service suppliers will generate incremental revenue exceeding $300 billion, mostly in services.

My boss said to me a few times in late 1980's, "technology has its place, its place is not everywhere." I don't think he will say it now.

Questions that need to be asked: How is reliability measured? Who will measure it? Who will assure it?

I & IT STAKEHOLDERS

The parties with interest in the reliability of I & IT include users, systems developers, management and regulators. Users in turn include customers, employees and trading partners. In the public sector, citizens are customers. These stakeholders have varying degrees of reliance on systems and influence over systems reliability.

WHAT DOES SYSTEM RELIABILITY MEAN?

Reliability in an information system must encompass the following five attributes: completeness, authorization, accuracy, timeliness and occurrence. Occurrence includes existence, e.g., recorded transactions actually occurred, or recorded assets actually exist. One can use the acronym CAATO to memorize these attributes. These attributes should be related to the entire transaction cycle, which includes input, processing, output and information storage. This cycle applies to systems that handle and record transactions as well as systems that are used mainly for producing information. In the latter case, a transaction would be a request for information or a system generated report.

Combining the CAATO attributes with the transaction cycle, one would expect a reliable system to have the following performance:

- It processes transactions completely.
- It provides complete and relevant information to users to meet their requirements.
- It has adequate resources and controls to prevent loss of stored information.
- It accepts only authorized transactions.
- It releases information only to authorized parties.
- It changes information only based on authorized requests.
- It processes transactions accurately.

- It performs regular checks and reconciliations to ensure accuracy of stored information.
- It provides accurate information to users.
- It processes transactions promptly.
- It provides current information to users as needed.
- It processes only real transactions (transactions that have actually occurred).
- Its information reflects only real transactions, assets and liabilities, i.e., revenue, expenses, assets and liabilities as indicated in the system actual exist.

How about confidentiality? A system is not reliable if it does not protect confidential information. Well, that is really part of authorization. How about availability? A system is reliable only if it is available when needed. That is accounted for under timeliness.

A growing concern is security. Security is a component of system assurance that is addressed as part of authorization. A secured system means that access is always authorized.

HOW IS RELIABILITY ACHIEVED?

A system does not satisfy the above criteria by chance. It needs checks to make sure transactions are processed and information is produced to meet the completeness, authorization, accuracy, occurrence, timeliness and efficiency attributes. These checks are called internal controls. Why do we call them internal controls, rather than just controls? Controls may be external, e.g., monitoring by creditors or regulators. Although external controls serve to mitigate risks, the organization operating the system has little influence over external controls. Therefore, organizations should rely mainly on controls that they can influence, i.e., internal controls implemented by the organizations themselves.

Internal controls may be manual or automated. Implementing internal controls assures stakeholders that systems are reliable, i.e., they have the characteristics of completeness, authorization, accuracy, timeliness, occurrence and efficiency. On an ongoing basis, stakeholders will want assurance that the system continues to be reliable, i.e., internal controls continue to work properly. Such assurance can be achieved by testing controls.

Internal controls should be applied to the following five system components: infrastructure, software, people, procedures and information.

Infrastructure includes real estate, the network and hardware. They have to have enough capacity, continuously available and be protected from sabotage, abuse, malfunction and unauthorized access. These components need to be configured in such a way that working together, they provide the platform for reliable information processing.

Software includes system software and application software. System software refers to software needed to interface directly with the hardware, e.g., the operating system It also includes database management systems which support multiple transaction processing applications. Application software means systems that process transactions directly or produce end user information. Application software is run on system software which in

turn interfaces with hardware directly. Software has to be rigorously developed, tested and documented. It also has to be monitored to detect glitches and protected from unauthorized changes.

People include management, systems developers, technology infrastructure staff like system administrators, and users. A system administrator is someone who controls the software implementation in a computer, usually a server. This person has full control over the computers that s/he supports. System administrators have powerful information access and pose a significant risk to organizations. They need to be rigorously controlled. We will discuss this further in Chapter Three.

Procedures include policies, standards and procedures for employees and customers. They have to be concise, current and well communicated. Change control should be applied.

Information is the most critical component of a system as without information, a system does not serve its purpose. It is information requirement that determines the extent and type of infrastructure, software, procedures and people. Each system should be tagged to be owned by an executive and it is up to that owner to assess the criticality of information that in turn will affect the amount of money to be invested in the system. Organizations should have guidelines for executives to do such assessment. We will discuss this in more detail in the next chapter.

Information

Although information seems easy to manage compared to software and hardware, it is the most important component of a system. It was an argument I often had with systems developers when I was a young auditor. Hardware and software are no doubt more complicated than information and usually more expensive. However, the type and extent of hardware and software needed depends on what information the system is intended to process and in turn produce. Senior management should assign each system to be "owned" by an executive and charge that owner with assessing the criticality of information as a basis for deciding on the hardware and software as well as the internal controls to be applied to the system.

Traditional Information Structure

Information is organized in a system to describe entities and the attributes within each entity. For example, a payroll master file contains semi-permanent information of each employee such as employee number, name, position, salary, tax deduction code, name of supervisor, work location, date of hire, date of birth, year-to-date gross pay, year-to-date deduction for each type of deduction and year-to-date net pay. This file describes the entity called employee. Each record contains the information of each occurrence of the entity, e.g., each employee. The date of hire and salary are attributes that describe each occurrence of the entity, i.e., in this case, each employee that belong to the entity "employee". The term master file refers to a file of semi-permanent information. Each pay period, a transaction file is produced to record, for each employee, the gross pay, deductions and net pay. For each master file, there are multiple transaction files, which

are used to update the master file. Another example of a transaction file is a file of salary changes during the period. A transaction file contains a history of transactions and master file contains the current status information of members of an entity.

The above describes a conventional information structure in a system. The data files in each system pertain to only that system and are accessible to only that system. Each file should have a field that is used as the primary key. A primary key is a field that uniquely identifies a record, e.g., student number in the student master file qualifies as a primary key.

Database

A database is a collection of related data files. Databases are increasingly used in organizations to facilitate data sharing for real time transactions and data mining. However, as is common when efficiency is to be gained, risk can go up. The sharing of data files (tables) increases the potential access points and the complexity of software. Thus, organizations need to implement controls to mitigate the additional risks. Modern databases typically use the relational or object oriented relational model. Relational is the most popular model for systems that process primarily numerical and text data. This allows any two tables with a common attribute to interrelate and thereby provides more flexibility to analyze and correlate data. For example, the customer order transaction file can be correlated with the customer master file, using the customer number as the common attribute, to compare the sum of the current balance owed by a customer and the amount of the customer order to the credit limit, to decide whether to approve the customer order.

A table is visually identical to an Excel spreadsheet, regardless of the database management system. Common relational database management systems are Microsoft's Structured Query Language (SQL) Server and Oracle. Microsoft also has a mini version of relational database management system (RDBMS) called Microsoft Access. IBM's DB2, which predated PCs, is still the most popular RDBMS for Z series servers (mainframe computers).

Relational database systems can also support objects. An object may be a picture, a sound clip or a video clip. It may also be is a piece of reusable object code that often contains standard data like font and color. It can also contain holders for users to input data, thus combining code and data in one object with the data portion being dynamic. When data is changed, a new object can be created. Object code means computer program(s) that have been compiled to machine language understandable to the operating system. Object code is compiled from source code using a compiler (software tool) specific to the source programming language like C++ and an operating system like Windows.

In a relational database, two tables can be related if they have a common alphanumeric field, i.e., a field that can be used as a primary key. This field will be the primary key in one of the tables and will be a field in another table without being a primary key of that table. For example, an inventory table uses the product number as the primary key and among other fields, it has a supplier number. The supplier number is the primary key in

the supplier table. These two tables are said to be related which means a transaction can be used to update both tables and also queries can be made on both tables simultaneously. The supplier number field in the inventory table is called a foreign key because it is used as a primary key in another table. The foreign key of a table should not be blank, e.g., a product must have a supplier. The database administrator can configure the RDBMS to enforce that a foreign key must not be blank on any record; this is called referential integrity.

A new model, called non-relational database, NoSQL, is increasingly being adopted for large scale but less structured data analysis where precision is less important than speed and comprehensive coverage, e.g., for data mining, big data analysis as well as mobile applications involving audio and video streaming. It is less structured and reliable than the relational model but also more dynamic. It is the latter characteristic that makes it attractive for mobile applications. NoSQL is not used for business transaction processing, where precision overrides speed and comprehensiveness.

Common Reasons for Adopting a Database

1. *Broadening customer service*
   By sharing data between applications, transactions that span different business areas can be processed readily. For example, some bank customers have an automated overdraft protection arrangement with their banks. Under this service, if a customer accidentally overdraws a checking account, the checking account system will check the customer's savings account to see if there is enough money to cover the overdraft plus a small service charge. If so, without human intervention, the checking account system will move the money into the checking account. This avoids an NSF check. Without a database, the checking account files are "owned" by the checking account system and the savings account files are "owned" by the savings account system. It would be impossible for the checking account system to move money from the savings account system. This sharing of tables (files) between systems is called data program independence.
2. *Data sharing to expedite transactions and mitigate risk*
   Information is power. Organizations can empower systems and people by sharing information. For example, payroll information can be shared with the production system to expedite the accumulation of work-in-progress costs. Similarly, transaction history and holdings about deposits can be accessed by the loan system to decide whether to approve a credit application.

3. *Data mining*
   Some have said that computing power doubles every year. This is not an overstatement. A one-gigabyte portable hard disk as big as a shoe box cost $400 in 1998. With increasing computing power, organizations are performing more data analysis to know more about their customers, products and the markets. Without databases, analysis would be limited and less timely because correlation would require

more system administrator and programmer intervention. Data mining is the principle technique in customer relationship management systems that uses mathematical analysis of a mass of data from different systems that share a database.

4. *Reducing data redundancy*
   Without a database, a customer's address may be stored in three files if the customer has a checking account, a savings account and a personal line of credit. A database can create a separate file containing non-financial information such as the address which can be accessed by different systems when the address is needed, for, say, statement mailing. This reduces the time to update information, saves storage and avoids data inconsistency, e.g., the address in the savings account system is different from the address in the checking account system due to a data entry error when the address was changed. . While one may argue that the above savings will be offset by the increased computer time to search data from different files and in configuring the RDBMS, such increase in computer time, from experience, is more than offset by the savings in people time and the reduction in risks of data inconsistency.

5. *Increasing Computer Program Flexibility*
   Without a database, the data files of a system are "owned" by the system. For example, the checking account data files reside within the checking account system and only checking account programs can use these data files. This way, the computer programs have to keep track of the data file layout, i.e., what fields are in each file as well as the format and order of the fields. A database will alleviate programmers of this tedious work by providing a data dictionary that keeps track of the file layouts. A program only has to refer to the file (table) name and field names, instead of specifying the location and format of the fields when accessing a file. This increases programming efficiency and flexibility, as programs in one system can access the files in another system.

The person who controls a DBMS is called a database administrator (DBA). A DBA has powerful access and must be carefully screened before being placed on the position and must be rigorously monitored. A DBA must not be a system administrator so as to limit the power possessed by a single person. Limiting such power is called segregation of duties.

Data Organization Structure and Access Methods

A database consists of tables. A table describes an entity. Examples of entities are student and customer. Each table has multiple records which represent occurrences of the entity. For example, in the customer master table, each record represents a unique customer. Each entity has attributes like customer number and credit limit.

The records in a table may be stored sequentially based on the primary key. This is a controlled way to keep track of records. As records are added or deleted, it may not be necessary to sort the table. However, periodically, each table should be sorted to account for gaps and duplicates.

When a record is updated or needed for reporting, the DBMS or transaction processing system (if a database is not used) will find the record. The traditional method of finding a record is to start with the first record and compare the primary key value of each record to the primary key value of the record that has to be updated, e.g., comparing the customer account number of every record to the customer account number specified by the customer or a customer service representative. This is time consuming. Data architects many years ago came up with the index sequential method to overcome the inefficiency. It uses an index similar to that in a telephone directory. One column of the index contains the ranges of primary key values. The second column contains the physical location of the range of records that corresponds to each range in the index, e.g., disk 1, cylinder 5. This way, instead of searching record by record, the DBMS searches index first to narrow down to the range of locations where the desired record is. Index sequential is mainly used in old legacy systems. I say "old legacy" because the "less old" legacy systems have long been converted to use the direct access method. A common index sequential access software tool is IBM's Virtual Sequential Access Method for mainframe computers.

A faster method is called direct access method. The DBMS uses an algorithm to calculate the physical location of the record based on the primary key. How does this work, because records may be moved from time to time? Well, all record movement is controlled by the DBMS when a database is used. The DBMS uses an algorithm to calculate the location where a record will be placed before placing the record. Thus, using the same algorithm to calculate the location of the record to be updated is foolproof. The algorithm uses the primary key of a record and other information about the storage media like number of cylinders and tracks to calculate the physical location. The algorithm has to be sophisticated enough to prevent collision, i.e., two records having the same physical address. A drawback of this prevention is that the algorithm tends to be conservatively rigorous in calculating address space to prevent duplicates and in so doing may leave some physical disk space always vacant.

If there is collision, the DBMS can use the algorithm, the primary key value of the existing record and the physical address of the existing record to calculate a new address and move the physical record there. The new address will be located in a separate region of the database called a chaining region. The originally calculated address (which is occupied by an earlier record) will be used to store a pointer to the chaining region, without disrupting the existing record.

In some business systems, most records are updated periodically at fixed intervals, e.g., payroll. In this case, using the sequential method to update records is acceptable because most of the records have to be accessed in one pass anyway.

Management and auditors should perform checks to account for gaps and duplicates. In addition, checks and tests should be performed to validate the index and the direct access algorithm periodically.

Hardware

Today's information processing hardware can be conveniently classified as servers, personal computers, smart phones and routers. It is important for management to understand the capability of different hardware and its vulnerability in order to make cost effective procurement decisions. It is also important for auditors to be knowledgeable about hardware in order to assess risks and controls. We will describe the different types of hardware from a business perspective.

Servers

Servers come in different sizes; however, the two main types are Z series servers that support legacy systems and local area network (LAN) oriented servers. The former is run on the IBM's z/OS operating system. These servers used to be called mainframe computers because of their large size in memory and disk storage. As LAN oriented servers grow in size, the fast computing that was once the monopoly of mainframes is now affordable using LAN oriented servers. Although there is still some difference in speed and power between these two types of computers; the difference is becoming narrower and narrower.

The data architecture is different between PC based servers and Z series servers, as is the data format at the operating system level. For data representation, PC based servers use American Standard Code for Information Exchange (ASCII), which is more user friendly for PC users. Z series servers use Extended Binary Coded Decimal Interchange Code (EBCDIC), which contains a larger character set and therefore can accommodate a keyboard with more special keys. The operating system used in Z series servers is z/OS. Z/OS is viewed by some as a safer operating system than Windows mainly because it is a less popular target for hackers.

Servers should be in locked rooms. There should be a restricted list of computing devices connected to a server. People with direct access to a server, e.g., logging on a server directly to run operating system commands, should be highly limited with explicit management authorization. Servers are often reassigned between business areas and business systems so it is critical for management to keep current inventory by serial number and model as to their location, network connection and supported business systems.

Many organizations are optimizing the use of servers by deploying virtualization technology. This involves using software to dynamically allocate idle server hardware capacity to other busier servers to make the infrastructure more flexible to surging transaction volume. Virtualization also reduces hardware cost and the cost of hiring people to operate servers. It, however, increases the risk of business interruption as there is now more reliance on fewer servers.

Personal Computers

These are often called workstations, desktops, laptops, notebooks, notepads or tablets. They vary in size, speed, memory space and storage capacity. It is critical for management to have an approval process for assigning PCs so that employees are given only what they need. It is not uncommon to find that some employees possess multiple computers that are not all needed. It is also critical to have procedures to ensure that inventory of location, user and network connection of each PC is maintained and regularly updated. A common control is to require managers to sign off the list of computers assigned to their staff members at least annually and subject these lists to independent audits.

Smart Phones

Smart phones can be used to access servers directly to launch applications and retrieve stored data. They should be controlled at least to the same extent as that for personal computers and notebooks. In addition, because of the risk arising from mobility, more stringent controls should be applied to prevent unauthorized use, improper personal use and information leakage in transmission We will discuss these controls in more detail in Chapter Eight.

Routers

A router's main function is to collect information from client computers like personal computers and smart phones and routes them to servers. This alleviates the need to physically connect each client computer to a server, which may be difficult logistically. It also provides flexibility for a client computer to access different servers from time to time. All it takes is to change a router table and connect a router to the another server. A routing table describes the client computers and servers connected to the router. A router can be connected to multiple clients and servers. It is the "go between" for client computers and servers. The routing table must be protected from authorized change and kept current in relation to client requirements.

Software

There are two broad types of software: system software and application software. System software refers to software needed to interface directly with the hardware, e.g., the operating system. It also includes database management systems which support multiple transaction processing applications. Application software means systems that process transactions directly or produce end user information. Application software is run on system software which in turn interfaces with hardware directly. Software has to be rigorously developed, tested and documented. It also has to be monitored for malfunctions and protected from unauthorized changes.

Operating System

A computer cannot function without an operating system. This system software interfaces between transaction processing programs and hardware. It manages the allocation of hardware memory, disk space and the central processing unit (CPU). In PCs, the CPU is in a chip. The CPU is the hardware brain of a computer that can perform addition, subtraction, multiplication, division and comparison without the aid of software. The operating system can be configured to log activities and allow only certain activities. It also controls access to transaction processing programs (applications) and data files. The operating system also interfaces between other system software like a database management system (DBMS). It is important for every organization to have a policy and supporting procedures with respect to the operating systems that should be used in relation to business units and hardware types, version control and how each operating system will be configured for each computer. For example, once an organization has decided to adopt Windows 8, it should also adopt a standard blue print for configuration so that the logging features, allowable types of programs and file controls are consistent from computer to computer. We will discuss this further in Chapter Eight and Chapter Nine.

Applications

An application is a business system, as opposed to system software. There are four types of applications: batch, online real time, online input but batch update and eBusiness. They differ in terms of responsiveness, cost and risk. Most organizations use all four types of applications.

A batch system records transactions in batches instead of at the time they occur. Almost all organizations use this type of applications. For example, banks are known to have efficient online systems, yet they still use batch applications. Payroll in a bank is a batch system. Check clearing is also a batch system, i.e., if I write a check, the money does not come out of my account when the payee deposits the check. My account is charged only on the night the check is deposited. A batch system does not provide instantaneous response to the parties to the transaction mainly because such response is not required. A batch system runs a higher risk of incomplete processing because transactions are batched and input usually only once a day and in that process a transaction document may be lost. A batch system, however, is more secure because only a small number of people have access to input transactions, i.e., the parties to the transactions do not perform the data entry. A batch system also has better audit trail because there are usually more source documents. It also allows more time for users to detect errors before the errors are input to the system.

Some systems take data input in real time but the transaction is processed only at the end of the day along with other transactions of the same type that have been input throughout the day. This is because timing within a day is not of the essence. For example, a customer service representative may take my new address on the phone and key it in. The system may just store the data entered and then update my address in the master file at night. This is because my bank does not need to use my address during the day. A system that takes data entry online but updates the master file in a batch gives more assurance

about completeness than a batch system as a transaction is accepted by the system as soon as it occurs. It has a greater security risk because there are usually more people who have online access. There are more people with access because the objective of online data entry is to expedite data entry instead of routing the transactions to only a few people to enter in batches.

More and more systems are now online and real time, e.g., banking and point of sales. An online, real time system carries higher assurance of completeness than batch processing because transactions are entered as they occur, however, the risk of unauthorized access is higher because there are a lot of access points. Also, there is less chance to detect errors as there is less paper audit trail. An online system typically uses a database in order to provide comprehensive and real time response to users. Most online users like customer service representatives should not have to sign on to multiple systems to obtain the data when talking to a customer on the phone; this is a common reason most online systems use databases.

Batch and online are the two common ways of processing transactions in terms of immediacy. Another pair of alternatives is centralized vs distributed. Centralized processing means all transactions are processed in a central location, e.g., checks presented in a bank are sent to the data center only once a day for collection from the drawee banks.

Transactions can also be processed in a distributed manner, like automated teller machine (ATM), where some functions are handled locally at the ATM, e.g., identification of the bank code for service charge determination; whereas other functions are carried out centrally like checking whether the card has been reported lost. Typically, online real time systems process transactions in a distributed manner. Distributed processing has higher risks of unauthorized access and incorrect processing because more computers are involved in processing and thus software changes have to be implemented in more computers. Also, the system is more complicated as it has to keep track of what is processed centrally and what is processed locally.

An eBusiness system is an online real time system that runs on the Internet or an intranet. The risk of unauthorized transactions is even higher because there are almost infinite people with access. We will discuss eBusiness in Chapter Five.

Enterprise Resource Planning Systems

This is an integrated accounting system that links the common accounting functions to provide online update to multiple accounting journals and ledgers in recording each transaction. It minimizes data entry and printing by providing real time information to customer service representatives, accounting staff members, managers and system users. This expedites customer service, transaction processing, decision making and management reporting. The needed information comes from the system directly instead of being conveyed in email, phone calls and meetings, thereby also reducing the risk of misunderstanding. Two common commercial products of enterprise resource planning systems (ERP) are SAP and Oracle (not the same as the Oracle DBMS).

Going from more or less "stand alone" accounting systems to an ERP produces efficiency gain for the organization and standardizes the processes for data input, interpretation and output; standardization will help to prevent inconsistency and errors. This is a main reason organizations adopt ERP. However, standardization also calls for change and an organization adopting an ERP has to realize that. The upfront cost is high and payback may not come for several years. Such a project carries a higher risk than developing a stand-alone system. An ERP allows organizations to put in better internal controls because one control can be applied to several business areas and ERP vendors have included best practices in their design. Because of the wide scope of an ERP, an organization planning to implement it should seize the opportunity to review the business processes throughout the enterprise and establish a value chain of functions of activities while at the same time weed out or streamline the functions and activities that do not deliver value. An ERP should be used to automate and integrate efficient processes instead of magnifying inefficiency.

RESPONSIBILITY FOR SYSTEM ASSURANCE

Because internal controls carry a cost, they should be developed and implemented based on risk assessment. Risk assessment involves understanding the business and assessing the business impact of unreliable systems. Many would agree that the chief information officer is not the best position in an organization to assess the business impact of system failure for every system; in other words, the CIO is not expected to know each business product or service intimately, especially in a large organization.

The person who should be responsible for risk assessment of a system should be the executive responsible for the business affected. For example, if an ATM system goes down, the bank will lose revenue and customer goodwill. The board of directors will not be happy but because they are not employees they cannot carry out line responsibilities, their function is to provide oversight and make strategic decisions; so they cannot be charged with preventing and fixing such a system problem. The chief executive officer and chief operating officer would not be happy but they cannot attend to every problem; they operate at a strategic level. Well, going down the line, it would be logical to turn to the executive responsible for delivering the ATM banking service. That person has a business target to meet in terms of ATM revenue and profit. That executive is the "owner" of the ATM business and responsible for sourcing the processes to deliver the business, including the ATM system. This person has to assess the risks of ATM outage and errors and develop internal controls based on such risk assessment. In practice, s/he will use technical people and professionals in the bank to do the risk assessment and control development; but s/he will be the person the CEO turns to for ensuring that the ATM system is reliable.

Some might challenge that the executive accountability for the ATM banking service should not own the system but instead, the CIO should own it. Their rationale is that technology advance gave birth to ATM. Well, if we apply this reasoning, the CIO could be charged with owning all business systems. That is impractical and the business executives would likely disagree. Whether it is technology that drives business or business vision that drives technology deployment is like the chicken and egg problem.

Instead of fixing a point on this, we should keep in mind that information technology is a business enabler. The CIO is a technical support executive and a facilitator, but not a business owner.

Once the business owner has assessed risks and implemented internal controls for a system, that person should document and acknowledge that as the business owner for that system, s/he has assessed risks and implemented sufficient internal controls to reduce risk to an acceptable level. This executive should also apply a process to periodically review risks and controls in the system and then update the written acknowledgement. A control conscious organization would require documented risk acceptance from each business owner. The organization should have a framework and criteria to guide executives in risk assessment and acceptance.

Where a system is used to support more than one business unit, the CEO may assign "business ownership" of the system to the executive with the biggest business stake or the highest expertise in the system. For example, the chief financial officer should own the accounting system, and the vice-president of human resources could own the payroll system. Some systems do not process transactions and instead, provide a common service in the organization, e.g., email. Such a system would be logically "owned" by the CIO.

System owners, through technical and operations staff, design, implement and operate internal controls to *ensure* that risks are mitigated to an acceptable level. These owners should also carry out periodic assessment of controls to *assure* senior management and stakeholders that systems are reliable. Auditors periodically carry out audits of controls to independently *assure* their clients and auditees that systems are reliable.

At a corporate level, ultimately, the CEO is responsible for assuring its shareholders, customers and regulators that operation is reliable and that customer information is processed correctly and protected from unauthorized access. More and more large organizations include internal control description in their annual reports.

BUSINESS CRITICAL SYSTEMS

Organizations always have limited resources. They should focus assurance effort on business critical systems. The criteria for business criticality for a corporation addresses mainly profitability and customer service. The criteria for a government include safety, health, welfare, revenue and expenditure control. The criteria for a university would include education quality, faculty support, revenue and expenditure control. We have listed here, for general reference, a list of systems that organizations should consider to be business critical. We will use three types of organizations as examples to show the common business critical systems: retail business, banks and governments. These are by no means complete lists of business critical systems. Each of these systems can be broken into subsystems. The term "mission critical systems" is also commonly used. Some people think that mission critical systems are more important than business critical systems. However, in closer analysis, a business critical system could cripple an organization if it is out for a few days. Just recall what you did or could not do last time

email was down. By identifying and prioritizing business critical systems, one can address the significance of mission critical systems. In other words, a mission critical system is a business critical system with high priority, or we can call it a tier 1 business critical system.

A large organization should have a register of systems ranked by business criticality. Each system should be assigned to an executive for ownership. The owner is accountable for the system's reliability.

The following are common business critical systems.

Manufacturers, wholesalers and retailers

Accounting

Costing

Customer relationship management

eBusiness portal

Electronic data interchange

Expenditure control

Fixed asset

Franchising

Inventory

Payroll and human resources

Point of sales

Radio frequency ID interfaces

Sales

Stores profitability

Supply chain management

Treasury

ERP (would encompass a number of the above functions)

Financial Institutions

ATM

Accounting

Branch profitability

Brokerage

Credit card

Customer relationship management
Deposits
eBanking portal
Expenditure control
Financial derivatives
Financial service regulatory reporting
Fixed asset
Insurance underwriting
Loans
Mortgages
Non-interest revenue
Payroll and human resources
Portfolio risk management
Treasury

Governments
Accounting
Citizenship and residency identification
Court administration
Educational institutions financing and monitoring
eGovernment portal
Expenditure control
Family support (child care and alimony enforcement)
Fixed asset
Health insurance
Payroll and human resources
Police
Supply chain management
Taxation
Transportation safety and licensing
Treasury
Water supply
Welfare

CURRENT IT ISSUES

Chartered Professional Accountants Canada and American Institute of Certified Public Accountants conducted a survey of top technology initiatives in 2013. Here is the list of the top ten initiatives.

1. Managing and retaining data
2. Securing the IT environment
3. Enabling decision support and analytics
4. Managing IT risks and compliance
5. Governing and managing IT investment and spending
6. Leveraging emerging technologies
7. Ensuring privacy
8. Managing system implementation
9. Preventing and responding to fraud
10. Managing vendor and service providers

Managing and Retaining Data

We are in the age of information overflow and the Internet is a significant contributing factor. There is no doubt in anyone's mind that information can convey power. However, information can also weaken an organization if it is wrong or irrelevant. Irrelevant information can waste processing resources and lead to inappropriate decisions. Computing power doubles every year. This is a two-edge sword to information management.

With vast computing resources, organizations tend to collect, share and retain increasing information. This can lead to information overflow that results in inefficiency, misuse and mistakes. On the other hand, organizations can use growing computing power to perform more thorough information analysis.

The world is increasingly information intensive. Some people say we are in an information revolution. It is critical for an organization's success to capture the right information, propagate information and knowledge to the right people, codify information for consistent retrieval and interpretation and to classify the risk of information for determining the extent of controls. This requires a formal program of policies, software tools, procedures and training. A large organization should have an information management department whose function is to set the policies and standards for information management, provide the relevant training and coordinate information risk assessment.

Securing the IT Environment

This topic has made the list every year in the past ten surveys conducted by Chartered Professional Accountants Canada. It will be increasingly challenging with cloud computing, open networks, mobile computing and outsourcing. There are security breaches in the news every week.

An organization that has not considered all the vulnerabilities and threats related to information technology, and has an inadequate security policy, could be a serious risk. The loss, theft or compromise of a mobile device could disrupt an organization's operations and result in the loss of sensitive or confidential client and customer data. A cyber attack could have the same consequences.

Enabling Decision Making and Analytics

The reports provided to management should be aligned with an organization's strategic goals. However, this may not be the case if the organization's data architecture does not support an effective reporting system. As a result, management may receive inaccurate or incomplete reports, and, consequently, may be at risk of making poorly informed business decisions.

Management must put in place a rigorous and formal structure of data analysis to provide business intelligence. This structure should include advanced tools for data collection and data mining. Organizations should take advantage of the exponential growth in computing power to broaden and deepen their analysis of business data. Some major data analytic firms count large Fortune 500 companies and government agencies among their clients by providing advanced analysis of customer, investor and taxpayer data. It is important for such companies that outsource data analytics to ensure confidentiality of raw data and the resultant business intelligence. It is equally important for organizations to educate their managers to interpret the analyzed data properly in light of the business objectives, and to address the business intelligence in their risk management programs. The risk management program should use the analyzed information to better assess business risks; on the other hand, new products, new services and business decisions arising from the business intelligence should be subject to risk management review to avoid being misled by or overreacting to the output of complex algorithms. Banks started hiring PhDs in mathematics more than two decades ago to help improve their fixed income portfolio and design financial derivatives. However, during the financial crisis in 2009, the CEO of a major North American bank said that the bank had no shortage of mathematicians, and that it could have used more PhDs in psychology. In quite a few banks, the use of mathematics to design financial products seemed to have gotten carried away.

However, the direction is definitely to analyze more information to continuously fine tune the customer relationship system, risk management and business intelligence. Big data analysis is just starting and will grow fast. Quantum computing development will go hand in hand with this and be an important facilitator. These require focus by the chief information officer, chief technology officer, chief knowledge officer and chief privacy officer. Big data means collecting large volumes of data beyond business transactions, that are somehow related to an organization's business in order to set more competitive strategies and make better informed corporate and business development decisions. Some organizations are finding that big data is testing their relational database management systems to the limit and are also adopting the NoSQL model. NoSQL is more flexible but

can be less precise. Big data is not used for transaction processing and because of the large volume of data being analyzed, a slight compromise in precision is not detrimental, when it is in favour of comprehensiveness.

Managing Risk and Compliance

Businesses have always had to deal with regulatory compliance. However, in the last 10 to 20 years, these requirements have increased and been drawing more media attention. A number of factors have contributed to this trend. They include the Internet, privacy and increasing public reliance on business financial health. Looking deeper, one can tie all these factors to the Internet. The Internet has changed the world.

The Internet has accentuated privacy concerns, and this has motivated more governments to increase privacy legislation enforcement. The Internet has expedited global data flow and communication, and this makes it easier for investors to learn about public companies and therefore more likely to invest in public companies, and therefore rely more on public companies' financial health. The Internet allows organizations to share their networks and open their systems to affiliates as well as trading partners. This has lowered the cost of computing and made mergers and acquisitions more attractive. Increasing mergers and acquisitions mean larger corporations and that raises concerns about the assurance that transactions, information and business relationships are at arms-length, transparent to investors and reliable.

Recognizing the increasing risk related to global competition and growing automation, governments and professional bodies have imposed legislations, regulations and accounting rules to ensure that business operations and financial disclosures serve the interest of customers, investors and citizens. Here is a common list of legislations, regulations and similar requirements that are imposed on large corporations:

1. Privacy acts – we will discuss this more in Chapter Five.

2. Sarbanes Oxley Act (SOX) – This U. S. legislation was passed in 2002 soon after the Failure of Enron and is intended to provide stronger assurance to investors about reliance on the financial health of public companies. Enron Corporation was an American energy, commodities, and services company based in Houston, Texas. Before its bankruptcy in late 2001, Enron employed approximately 22,000 people and was one of the world's leading electricity, natural gas, communications, and pulp and paper companies, with claimed revenues of nearly $101 billion in 2000. Fortune named Enron America's Most Innovative Company for six consecutive years. At the end of 2001, it was revealed that Enron's reported financial condition was sustained substantially by institutionalized, systematic, and creatively planned accounting frauds.

   The major features of the Act include requiring public companies to certify internal controls that support the financial statements and restricting the types and extent of consulting services performed by accounting firms to their audit clients.

The first requirement helps ensure that frauds are properly prevented and detected and that financial statements are reliable. The second requirement fosters auditor independence and therefore enhances the reliability of the audit opinion. Public companies have to document their internal controls and engage external auditors to provide an opinion on such controls. There is significant IT impact because internal controls in public companies are increasingly automated. SOX also requires a public company to disclose to the public on a rapid and current basis any material change in financial condition or operations. This calls for a rigorous set of internal controls to ensure timely and accurate reporting of financial performance within the company and to alert management of any adverse trend.

3. Investor Confidence Rules – This regulation was introduced by Canadian Securities Administrators (CSA) to reflect the major Sarbanes Oxley requirements. CSA is a voluntary umbrella organization of Canada's provincial securities regulators whose objective is to improve, coordinate and harmonize regulation of the Canadian capital markets. It aims to achieve consensus on policy decisions which affect the Canadian capital market and its participants. It also aims to work collaboratively in the delivery of regulatory programs across Canada, such as the review of continuous disclosure and prospectus filings. The Investor Confidence Rules require the CEO of every public company to certify the adequacy of internal controls that support financial statements to its provincial securities regulator.

4. Industry regulations like bank acts, insurance company acts and public utility regulations - These legislative requirements sometimes require system configuration or development. For example, the Affiliate Relationships Code for Electricity Distributors and Transmitters, published by Ontario Energy Board, revised on March 15, 2010, states the following in section 2.2.2.

> Where a utility shares information services with an affiliate, all confidential information must be protected from access by the affiliate. Access to a utility's information services shall include appropriate computer data management and data access protocols as well as contractual provisions regarding the breach of any access protocols. A utility shall, if required to do so by the Board, conduct a review of the adequacy, implementation or operating effectiveness of the access protocols and associated contractual provisions which complies with the provisions of section 5970 of the CICA Handbook. A utility shall also conduct such a review when the utility considers that there may have been a breach of the access protocols or associated contractual provisions and that such review is required to identify any corrective action that may be required to address the matter. The utility shall comply with such directions as may be given by the Board in relation to the terms of the section 5970 review. The results of any such review shall be made available to the Board.
>
> www.ontarioenergyboard.ca/OEB/_Documents/Regulatory/Affiliate%20Relationships%20Code%20for%20Gas%20Utilities%20ARC.pdf (accessed on January 2, 2015)

Section 5970 refers to the former Canadian Institute of Chartered Accountants Handbook Section 5970, which provided guidelines for accounting firms to conduct an audit of the internal controls of a service organization for assurance to the shareholders' auditors of user organizations. This guideline has been replaced by Canadian Standards for Assurance Engagements Section 3416, that serves the same purpose. We will discuss this in more detail in Chapter Ten.

5. Payment Card Industry Security Standards – This is discussed briefly under External Audits above. We will cover this in more details in Chapter Eleven.

Governance and Managing IT Investment/Spending

The term "IT governance" is often used in articles and conferences but many who refer to this term do not understand fully what it entails. Many think this equals the chief information officer's job description, just as many thinking that corporate governance is the CEO's job. A CEO needs the board's support and guidance to "govern" the corporation. S/he also needs the support of the chief operating officer, the chief financial officer, the chief information officer and other executives. Together, they develop and implement strategies and policies to lead and monitor the organization. Similarly, the CIO needs support of all these parties and the CIO's managers to deliver IT governance. IT governance has to be congruent with corporate governance and is a subset of the latter.

The September 2011 issue of Canada's CA Magazine defines IT governance as the oversight responsibility for the strategic and tactical management, planning and organization, acquisition and implementation, delivery and support, as well as monitoring and evaluation of the IT environment.

The board of directors is also accountable for IT governance to a considerable extent, although not in a hands-on manner. The board carries out its IT governance responsibility by approving major IT projects and monitoring the progress of major projects.

At a management level, an IT steering committee consisting of the C-suite (CEO, COO, CIO, CFO) and senior line executives should oversee and monitor the use of IT including approving major projects, being informed of major IT audit findings and demanding corrective actions. The objective of IT governance is to ensure that the organization has sufficient IT skills and tools to support its business in the medium to long term and that these skills and resources are used effectively and efficiently. IT governance also ensures IT is used right and the right IT is used. Although management naturally does not always think about internal controls, controls are necessary to ensure effective use of IT resources, and hence effective and reliable systems. It is important for management and auditors to continuously assess whether the governance process adequately addresses risks and includes internal controls. At this stage, the type of internal controls to be included consists of management controls, i.e., controls to be exercised by managers instead of operations controls.

Privacy

The public has never been more concerned about information privacy. The concern has been heightened in recent years by technology advances, identity theft and security breaches. The exponential increase in computing power allows organizations to store more and do more analysis of personal information, potentially breaching privacy.

Hackers are now more entrepreneurial. They are less interested in defacing a web site or sending a worm to bring down a web site without financial gain and running the risk of going to jail. They are more interested in stealing identities and selling to criminals.

Every system that processes or stores personal information is subject to privacy breach. Before such a system is implemented, the organization should conduct a privacy impact assessment and such assessment should be carried out regularly even after system implementation.

Managing System Implementation

An organization's strategic goals drive its system implementation. If the goals and the implementation are not aligned, the organization may only partly meet its business goals for implementation – or not meet them at all. It may not realize its return on investment for an implementation project, and it may have other problems such as converting or transferring data inadequately.

To manage system implementation, an organization establishes a strong alignment between its strategic goals and IT-related projects. In evaluating new projects, it considers the recommendations of internal advocates who know how to establish a strong business case for such projects. It analyzes and documents the business requirements for such projects, and it evaluates their value based on return on investment, earned value analysis and other criteria. Finally, it ensures the quality and integrity of project data.

Leveraging Emerging Technologies

New technologies are being introduced and adopted at a faster than ever pace by organizations and individuals. These come in the forms of new hardware, more sophisticated and faster software, advanced techniques in hardware virtualization like cloud computing that pulls the resources of idle computer resources on the Internet or an intranet, and social media tools like Twitter. New technologies promise productivity gain and more enriched information availability. However, they also present the risk of unauthorized access and can lead to incorrect information if the technologies and tools are not properly used.

Organizations should charge their CIOs with keeping in touch with technology development and assessing the applicability of new technologies. Such assessment should include risk analysis, i.e., the risk of not applying a technology and the risk of applying a technology prematurely or incorrectly.

Preventing and Responding to Fraud

Information technology has facilitated the perpetration of fraud in organizations. Those organizations that do not know how to identify IT related fraud, do not have policies to prevent such fraud, and do not have plans to respond to a fraud, are particularly vulnerable. Likewise, organizations are at greater risk if they do not have policies to prevent management override opportunities within financial-related systems. If a fraud does occur, these organizations may not have plans in place to respond.

To prevent and respond to fraud, an organization should consider the fraud risks associated with information technology, designs policies and internal controls to mitigate such risks, and establishes policies to detect management override abuse.

Managing Vendors and Service Providers

It is hard to find a large organization that does not outsource. Large organizations that have outsourced in varying degrees include financial institutions, retail giants, software vendors, governments and utility companies, pretty much in every industry. The main reason for outsourcing is to cut cost. But risk always goes up.

When an organization outsources, it stands to lose skills and in some cases the organization may have to share or give up intellectual property like computer programs. While outsourcing gives the organization short to medium term gain, it may lead to long term pain. Some people blame unemployment on foreign outsourcing. This is also quite prevalent in Canada. For example, a friend of mine working in a large financial services company has told me that most programmers in his team are working for a software service company in India which provides programming resources to this North American financial services company on contract. He worries that one day even he, as the team lead, will lose his job once the consultants in the IT service company have learned enough about how the system interfaces with business processes. There is a concern that over time, large North American companies may not have a core knowledge base in commercial and financial software development. Management has to consider this risk and also ensure that staff morale remains high by providing training and retaining the needed core competencies within the company.

Outsourcing also increases the risk of confidentiality and privacy as now another organization has access to the outsourcing organization's data. Sometimes a service organization in turn outsources, in which case, the risk of confidentiality breach is compounded.

When assessing and reporting on system reliability, management and auditors have to evaluate the risks of outsourcing and the adequacy of internal controls in the service organization. The latter may be complicated as the service contract may not require the service organization to exercise internal controls, may not give the user organization the right to audit the service organization, or may not specify the service organization's obligation to provide an independent control assurance report. It is important for such arrangement to be made before the contract is finalized. We will discuss outsourcing further in Chapter Ten.

MANAGEMENT CHECKLIST

To ensure that I & IT is reliable and cost effective, senior management should adopt the following practices.

1. Assign business executives to own information systems and infrastructures. Each system should have an owner. IT infrastructures would logically be owned by the chief information officer because an infrastructure usually supports multiple business systems.

2. Establish corporate policies and standards for information risk assessment.

3. Establish a process for periodic risk assessment, internal control formulation and internal control reporting to senior management and the board of directors.

4. Involve the board of directors in IT governance and ensure this is addressed at least twice a year in board meetings.

5. Establish a policy on the use of I & IT in the organization with respect to how to use IT as a business enabler and the approval process for IT investment.

6. Develop an IT strategy to be congruent with the business strategy. The IT strategy should consider the applicability of new technology.

7. Develop a process to continuously assess the cost effectiveness of IT applications.

8. Ensure that the job description and performance contract of each executive includes the appropriate I & IT assurance accountability.

Going forward, we will provide comprehensive discussion of I&IT assurance in the following chapters.

Chapter 2 – I&IT risks

Chapter 3 – IT governance and general controls

Chapter 4 – Systems development controls

Chapter 5 – Control and audit implications of eBusiness

Chapter 6 – Application controls

Chapter 7 – Data analysis techniques

Chapter 8 – Common access controls

Chapter 9 – Operating system access controls

Chapter 10 – SysTrust and Payment Card Industry control assurance engagements

Chapter 11 – Computer crime

CONCLUSION

The Internet has changed the world. Large businesses can act small by using the Internet to customize service. Small businesses can act big by using the Internet to reach the world. Although there is still a "digital divide" in the world, the difference between the "have" and the "have not" in knowledge access is narrowing, as information finds its way across continents instantaneously. IT empowers everyone to do constructive things and damage. Successes can be attained and catastrophes can be caused in great magnitude within a short time. Just look at how quickly some of the large IT companies have grown in a few years, and how some major financial transaction irregularities carried out in a few days involving computer systems that caused huge losses.

Continuing advance in technology makes systems reliability more important. In addition to putting in processes and infrastructure to ensure system reliability, management needs to continuously exemplify and promote a quality culture and hold everyone responsible for quality.

The pace of life is different than it was 10, 20 years ago. A study shows that walking speed has increased by 10% in the last 20 years. While technology empowers people to do more with less physical movement, technology also delivers more and more information and system functions and that makes people more inquisitive and ambitious. It is the quest for information to do things better that makes people more competitive and less patient; hence the pace of life has gone up. It is "keep up or give up". Systems undergo more frequent changes. System assurance has to keep pace.

Boards of directors have to continuously challenge their management about the sufficiency of IT assurance provided to the boards and customers. Users and customers should be educated to play a constructive role towards such assurance. Regulators need to monitor company system reliability in addition to checking the correctness of filed reports.

SUMMARY OF MAIN POINTS

System Assurance Criteria

- Completeness
- Authorization
- Accuracy
- Timeliness
- Occurrence
- Efficiency

System Components

- Infrastructure
- Software
- People
- Procedures
- Information

Types of Assurance Engagements

- Financial statement audit
- Value for money audit
- Internal audit
- Third party control assurance audit
- Audit for compliance with specific legislation or contract
- Forensic audit

Types of Systems

- Batch
- Real time
- eBusiness
- Centralized vs distributed processing
- Direct access vs sequential access
- Enterprise resource planning systems, uses database.

Current IT Issues

1. Managing and retaining data
2. Securing the IT environment
3. Enabling decision support and analytics
4. Managing IT risks and compliance
5. Governing and managing IT investment and spending
6. Leveraging emerging technologies
7. Ensuring privacy
8. Managing system implementation
9. Preventing and responding to fraud
10. Managing vendor and service providers

REVIEW QUESTIONS

1. Which system component is the most business critical and why?

2. How would you rank the system assurance criteria for a financial statement audit? For an internal audit?

3. Computing power doubles annually. How do you think this affects system assurance?

4. What are the criteria for assessing system criticality in a bank? A large retailer? A government?

CASE #1 – "Aging Information Technology Systems"

This case study is a direct extract from the Spring 2010 report of the Office of the Auditor General of Canada (OAG). Chapter 1 of the report, titled "Aging Information Technology Systems", is used in this case study. The following is an excerpt of Chapter 1 of the Spring 2010 report, including only the "Main Points" of the "Aging Information Technology Systems" report.

Source: Spring 2010 Report of the Auditor General of Canada – Office of the Auditor General of the Canada. *Reproduced with the permission of the Minister of Public Works and Government Services, Canada, 2012.*

What Was Examined

Aging information technology (IT) systems refers not only to a system's age in years but also to issues that affect its sustainability over the long term, such as the availability of software and hardware support and of people with the necessary knowledge and skills to service these systems. The term also relates to a system's ability to adequately support changing business needs or emerging technologies, such as 24/7 online availability.

The Treasury Board of Canada Secretariat, through its Chief Information Officer Branch (CIOB), is responsible for establishing the federal government's overall strategic direction for IT, in consultation with deputy heads of departments. It is also responsible for identifying areas that offer significant government-wide benefits and for leading initiatives to achieve government-wide solutions. According to the most recent figures available (for 2005), departments and agencies spend about $5 billion a year on IT.

We examined whether five of the government entities with the largest IT expenditures - the Canada Revenue Agency, Public Works and Government Services Canada, Human Resources and Skills Development Canada, the Royal Canadian Mounted Police, and Citizenship and Immigration Canada — have adequately identified and managed the risks related to aging IT systems. The audit also examined whether the Treasury Board of Canada Secretariat, and specifically its Chief Information Officer Branch, has determined if aging IT systems is an area of importance to the government as a whole and to what extent it has provided direction or leadership in developing government wide responses to address the related risks.

We also looked at three major systems that deliver essential services to Canadians — the Employment Insurance Program, the Personal Income Tax and Benefits Return Administration System, and the Standard Payment System — to determine how the responsible entities have addressed the risks related to the aging of the IT systems that support these services. The Employment Insurance Program processed more than 3.1 million claims and paid out over $16.3 billion to claimants in the 2008–09 fiscal year.

The Personal Income Tax and Benefits Return administration system processed more than 27 million income tax and benefit returns that provided $166 billion of revenue and also distributed $17 billion in payments for benefits and credits in 2008–09. The Standard Payment System (SPS) is the principal system the government uses for issuing payments, including Old Age Security, Canada Pension Plan and Employment

Insurance benefits. It issued more than 250 million payments in 2008. In about 60 percent of cases, these payments are the only income or the main source of income for the people who are receiving them.

Audit work for this chapter was substantially completed on 30 November 2009.

Why It's Important

The federal government relies heavily on IT systems to deliver programs and services to Canadians. Even though these systems are functioning, many of them consist of legacy applications that are supported by old infrastructure and are at risk of breaking down. A breakdown would have wide and severe consequences — at worst, the government could no longer conduct its business and deliver services to Canadians. Even applications that meet current business needs can be difficult and expensive to operate and may not be flexible enough to respond quickly to changes.

The renewal and modernization of IT systems does not happen overnight. It must be planned and budgeted for over the long term. The cost to renew and modernize IT systems are significant and can take many years to fund, and implementation can take five years or longer. Without sufficient and timely investments to modernize or replace aging systems, the ability of departments and agencies to serve Canadians is at risk.

What Was Found

- Aging IT has been identified as a significant risk by the five organizations we examined, and the majority of them consider it sufficiently important to include it in their corporate risk profiles. They state that if these risks are not addressed in a timely manner, the systems may not have the capacity to meet current and future business needs.

- Although the Chief Information Officer Branch of the Treasury Board of Canada Secretariat is aware that the aging of IT systems is an issue, it has not formally identified it as an area of importance for the government. Nor has it assessed the issue from a government-wide perspective or worked with departments and agencies to develop government-wide solutions. Despite the significant funding likely to be needed across government to renew aging systems — estimated at a total of $2 billion in three of the five entities alone — the CIOB has not formulated strategic directions or a plan to address these issues on a government-wide level.
- Citizenship and Immigration Canada, Public Works and Government Services Canada, and Human Resources and Skills Development Canada have taken some steps to manage the risks related to their aging IT systems, but much work remains to be done. The Canada Revenue Agency and the Royal Canadian Mounted Police are farther along. They have both identified the significant risks associated with their aging systems and completed a multi-year investment plan

that defines and prioritizes ongoing and future work. Based on their preliminary estimates, they have determined that the costs involved are significant and that presently they lack sufficient resources to complete critical investments.

The departments and agencies have responded. The departments and agencies agree with all of our recommendations. Their detailed responses follow the recommendations throughout the chapter, as applicable.

Introduction

1.1 Canadians expect the government to provide them with many services, such as processing personal income tax returns, issuing pension and benefit payments, and safeguarding personal information. Information technology is now a vital part of service delivery for the government. Government business is supported by a vast array of information technology (IT) systems, some of which have been in use for several decades. However, the term “aging IT systems” refers to more than just how old a system is in years. Many systems that are 10 years old or older were designed to be continuously upgraded. These systems are functioning and are likely to continue to do so for some time.

Risks relating to information technology systems

1.2 For the purposes of this audit, “aging IT systems” refers to applications and infrastructure that may be meeting current needs but are becoming increasingly expensive to operate and may pose certain risks. These risks may affect security or restrict the way the government conducts its business because systems cannot be easily updated to respond to changing business needs flowing from new laws, regulations, or industry standards. The most damaging risk is that an aging critical system could break down and prevent the government from delivering key services to the public — such as issuing income tax refunds and employment insurance and pension cheques. While these risks could apply to any IT system, they are more likely to affect older systems. Exhibit 1.1 describes some of the major factors that drive departments to modernize their aging systems.

Exhibit 1.1—Overview of major factors driving the modernization of aging systems

Factor	Description
Skills shortage	Fewer staff and contractors have the skills and knowledge to use older programming languages and source code structures.
Vendor support	Vendors may no longer exist or no longer support older products.
Regulatory compliance	Outdated systems may be hard to update to comply with changing laws, regulations, and industry standards.
Maintenance costs	Costs go up because aging systems are very complex and difficult to maintain, there are few service providers, and parts are scarce and often very costly.
Access to data	Information becomes increasingly cumbersome to extract and analyze as data structures age.
Meeting client expectations	Older systems cannot be modified to support modern technologies and meet expectations such as 24/7 availability and workflow.
Security	**Legacy systems*** cannot always be modified to conform to changing security requirements (for example, password complexity).
Green IT initiatives	Older IT systems are generally not energy efficient and are hard to modify to reduce their environmental impact.
Disaster recovery	The older the system, the harder it is to recover data after a disaster.
***Legacy systems**—Old technology, computer systems or application programs that continue to be used, even though newer technology or more efficient methods of performing a task are now available.	

*** End of OAG report excerpt****

Case Questions

1. What do you think are the causes of aging systems in the public sector?
2. Are these causes common in the private sector?
3. How do the risks of government systems differ from private sector business systems?

CASE #2 – NASA's IT Governance

This case study is a direct extract from a June 2013 audit report of the NASA Office of Inspector General, Report IG-13-015. The title of the report is NASA's IT Governance. The Overview has been included here.

Source: http://oig.nasa.gov/audits/reports/FY13/IG-13-015.pdf, accessed on January 7, 2014.

JUNE 5, 2013 AUDIT REPORT

NASA'S INFORMATION TECHNOLOGY GOVERNANCE

OFFICE OF INSPECTOR GENERAL

National Aeronautics and Space Administration

REPORT NO. IG-13-015 (ASSIGNMENT NO. A-12-018-00)

OVERVIEW

NASA'S INFORMATION TECHNOLOGY GOVERNANCE
The Issue

Information technology (IT) plays an integral role in every facet of NASA's space, science, and aeronautics operations. The Agency spends more than $1.5 billion annually on a portfolio of IT assets that includes approximately 550 information systems it uses to control spacecraft, collect and process scientific data, provide security for its IT infrastructure, and enable NASA personnel to collaborate with colleagues around the world. Hundreds of thousands of individuals, including NASA personnel, contractors, members of academia, and the public, rely on these IT systems daily.

IT governance is a process for designing, procuring, and protecting IT resources. Because IT is intrinsic and pervasive throughout NASA, the Agency's IT governance structure directly affects its ability to attain its strategic goals. For this reason, effective IT governance must balance compliance, cost, risk, security, and mission success to meet the needs of internal and external stakeholders.

In 2011, the Office of Management and Budget (OMB) issued a memorandum shifting the primary responsibilities of Federal Chief Information Officers (CIO) from policymaking and infrastructure maintenance to IT portfolio management. The memorandum mandated that Federal agencies equip their CIOs with authority over IT governance, commodity IT, program management, and information security.

For over 2 decades, NASA has struggled to implement an effective IT governance approach that appropriately aligns authority and responsibility commensurate with the Agency's overall mission. Since at least 1990, the Government Accountability Office (GAO) and NASA's Office of Inspector General (OIG) have highlighted a series of challenges stemming from the limited authority of the Agency CIO, decentralization of Agency IT operations, ineffective IT governance, and shortcomings in the Agency's IT security. Reports by GAO and OIG have noted that NASA has limited Agency-level oversight of its wide-ranging IT operations, and recently, the OIG reported that the NASA CIO could not fully account for the Agency's IT assets or ensure those assets complied with applicable IT security policies and procedures.

We initiated this audit to examine whether NASA's current IT governance structure appropriately aligns authority and responsibility to support the overall mission of the Agency. Specifically, we reviewed whether NASA's Office of the Chief Information Officer (OCIO) has the organizational, budgetary, and regulatory framework needed to effectively meet the Agency's varied missions.

Results

The decentralized nature of NASA's operations and its longstanding culture of autonomy hinder the Agency's ability to implement effective IT governance. The Agency CIO has limited visibility and control over a majority of the Agency's IT investments, operates in an organizational structure that marginalizes the authority of the position, and cannot enforce security measures across NASA's computer networks. Moreover, the current IT governance structure is overly complex and does not function effectively. As a result, Agency managers tend to rely on informal relationships rather than formalized business processes when making IT-related decisions. While other Federal agencies are moving toward a centralized IT structure under which a senior manager has ultimate decision authority over IT budgets and resources, NASA continues to operate under a decentralized model that relegates decision making about critical IT issues to numerous individuals across the Agency, leaving such decisions outside the purview of the NASA CIO. As a result, NASA's current IT governance model weakens accountability and does not ensure that IT assets across the Agency are cost effective and secure.

Limited CIO Control of IT Funding and Investments. We found that the Agency CIO had little control and visibility over the majority of NASA's IT budget. Of the $1.46 billion allocated for IT in fiscal year (FY) 2012, the Agency CIO had direct control of $159 million or 11 percent, the Centers had direct control of $393 million or 27 percent, and the Mission Directorates controlled the remaining $912 million or 62 percent. An anecdote recounted to us during our review illustrates the CIO's limited visibility and control of

NASA's overall IT spending. According to the Agency CIO, although planned IT expenditures for FY 2010 were $1.6 billion, the Agency actually spent $2 billion. However, the CIO was unaware of the $400 million in additional spending until the Mission Directorates reported actual expenditures to her office in a data call responding to an OMB request. We also determined that the Agency CIO's lack of authority over IT funding limits the Agency's ability to consolidate IT expenditures to realize cost saving and drive improvements in the delivery of IT services. With decreased budgets across the Federal Government and the reduction of NASA's IT budget by almost $1 billion since 2006, it is imperative that NASA find efficiencies in its IT operations, purchases, and investments.

Organizational Structure Marginalizes the Agency CIO. We found that NASA's organizational structure marginalizes the position and authority of the CIO. When NASA established the CIO position in 1995, it purposely limited the authority of the position to preserve control by the Mission Directorates and Centers over the IT assets related to their space, science, and aeronautics programs. Despite technological advances over the intervening 17 years and integration of IT into all Agency programs, the role of the NASA CIO has changed very little. Each Mission Directorate and each NASA Center continues to employ their own CIO and IT security personnel who oversee hundreds of independently operated networks and tens of thousands of computers and other IT hardware over which the Agency CIO has little control or oversight. Moreover, although the Center CIOs report to the Agency CIO, the Mission Directorate CIOs do not. We found that this partitioning of authority and control has not served the Agency well in terms of securing its IT systems or achieving economies and efficiencies in IT acquisitions and management.

NASA employs 1 CIO at the Agency level, 10 CIOs at the Center level, 1 CIO at the Jet Propulsion Laboratory, 1 CIO at the NASA Shared Services Center, and 1 CIO within each of the Mission Directorates. Having numerous officials with the same title and similar roles as the Agency CIO, some of whom do not report to the CIO, dilutes the CIO's authority and blurs the lines of accountability and responsibility for overseeing NASA's IT systems. Moreover, the Agency CIO is the only one of seven "Chief" positions at NASA that does not report directly to the Agency Administrator, a reporting structure that is out of line with Federal policy and best practices. In our judgment, affording the Agency CIO the same visibility as the other "Chiefs" would send a message about the significance of IT and better ensure that NASA's IT posture aligns with the strategic direction of the Agency.

The issues currently challenging the NASA CIO are not new and we and others have raised them repeatedly since NASA established the position almost 2 decades ago. While recognizing the problem, the OCIO has often advocated solutions that rely on "improved collaboration" between the OCIO, the Centers, and the Mission Directorates. While coordination and

collaboration are important components of any IT strategy, we do not believe they alone will be sufficient to overcome the significant and longstanding issues we and others have identified. NASA's diffuse responsibility for IT matters prevents the Agency CIO from taking and enforcing meaningful actions and instead, often reduces the position to issuing calls for increasing "cooperation and communication" – calls that at least up to this point largely have gone unanswered. In short, NASA's culture and current structure hinders the CIO's ability to implement and enforce new IT initiatives across the Agency.

Responsibilities and Interaction between IT Boards Unclear. In addition to the various layers of CIOs and associated IT personnel, NASA's IT governance structure includes three primary governance boards that report to the Mission Support Council (MSC) as well as numerous sub-boards and working groups. We found that the complexity of the board structure and a lack of documentation and training to explain the interrelationship of the boards has led to confusion among Agency IT personnel about the roles and responsibilities of the boards and diminished their value to the governance process. While the design of NASA's IT governance structure requires coordination and collaboration between the boards, in practice, IT managers are often unsure of the interrelation and function of the various boards and how decisions are intended to be made. Even though Mission Directorates are not required to utilize the boards for Mission specific IT decisions, the Mission Directorate CIOs cited time constraints, impact on Mission security, and potential non-approval by the Agency CIO as reasons to circumvent the board process. Moreover, NASA policy, including the charters for each of the boards, does not provide clear guidance or criteria for determining the issues or initiatives that must go before the boards for approval. As a result, NASA IT managers tend to rely on informal relationships rather than formalized business processes when making IT decisions.

CIO Cannot Enforce Security Measures over a Majority of NASA IT Assets. Over the past several years, our audits have repeatedly identified poor management processes and inadequate operational and technical controls that affect NASA's ability to protect the information and IT systems vital to its mission. Although the Agency CIO is responsible for developing IT security policies and procedures and implementing an Agency-wide IT security program, because the CIO lacks authority and control over Mission networks, the CIO is unable to enforce the implementation of IT security programs on a large portion of NASA's IT assets.

In 2012 Congressional testimony, the CIO acknowledged that the Agency's culture does not support building effective cyber security processes, and stated that the largest impediment to effective IT security is persuading and changing the Mission Directorate culture. Mission Directorates often fund their own computer networks and Directorate personnel are responsible for IT security, risk determination, and risk acceptance on those networks, limiting the ability of the Agency CIO to standardize those assets across the

Agency or ensure they adhere to security policies. Further, the OCIO's internal continuous monitoring function, the Security Operations Center (SOC), does not have purview over all of NASA's networks. According to the NASA IT Security Operations Manager, the SOC currently has visibility over approximately 90 percent of NASA's institutional networks but only over a very small portion of the Agency's Mission networks. As a result, the SOC relies on the Mission Directorates to self-report vulnerabilities and security incidents.

NASA's ability to secure its networks is further complicated because the Agency lacks a complete inventory of IT assets. For example, five Center CIOs told us they could not account for 100 percent of the IT systems and hardware at their Centers. Center Chief Information Security Officers (CISO) told us that the Agency's efforts to establish an inventory have been hindered by inconsistent enforcement of the policies and implementation of the tools meant to capture the information, pockets of resistance to providing the information, and inconsistent or lack of guidance from OCIO IT security management.

IT Governance across Government. Although NASA's mission is unique, the challenges the Agency faces in managing a decentralized IT environment are not. As part of this review, we benchmarked with IT officials at the Department of Interior, the Department of Veterans Affairs, and the United States Postal Service. Each of these organizations had a decentralized IT environment that was geographically diverse, independently operated, and that supported thousands of users. With support from Congress and agency leaders, each organization revamped their IT governance model and moved from decentralized IT systems to a more consolidated, centralized structure giving the CIO authority over IT budgets and resources agency-wide. Officials from each of these organizations reported that centralization – while time consuming and not without its detractors – has resulted in increased efficiency, security, and lower operating costs for their agencies.

Management Action

For almost 2 decades, the OIG and GAO have reported issues associated with NASA's limited CIO authority, decentralized IT operations, and ineffective IT governance. Although division of authority between Headquarters management, the Mission Directorates, and the Centers is historically the cornerstone of NASA's program and project governance, in our view mirroring this structure for managing IT purchases, operations, and security is no longer in the Agency's best interest. With mission critical assets at stake and shrinking budgets, NASA must take a holistic approach to managing its portfolio of IT systems.

To overcome the barriers that have resulted in the inefficient and ineffective management of the Agency's IT assets and operations, we recommend that NASA overhaul its IT governance structure to centralize IT functions and establish the Agency CIO as the top management official responsible for NASA's entire IT portfolio. Strong leadership by the CIO and OCIO staff will be required, but the CIO cannot make these changes alone. Rather, the NASA Administrator – backed by support and possibly additional resources from Congress – must be the driving force behind such organizational change. With the recent departure of the Agency CIO, NASA currently has a prime opportunity to reevaluate its IT organizational structure and personnel resources to ensure it is best positioned to meet its IT challenges.

Therefore, we recommend the NASA Administrator – in consultation with the Mission Directorate and Center CIOs and the Agency's senior management team – consolidate the overall governance of IT within the OCIO and ensure the OCIO has adequate visibility into Mission-related IT assets and activities. The Agency CIO should approve all IT procurements over an established monetary threshold that captures the majority of IT expenditures, regardless of procurement instrument. Additionally, the Administrator should make the Agency CIO a direct report and revise the job titles of the Center and Mission Directorate CIOs to more clearly delineate roles and responsibilities. Further, the renamed Mission Directorate CIO positions should directly report to the Agency CIO. We also recommend that the Administrator reevaluate the relevancy, composition, and purpose of the three primary governance boards in light of the changes made to the IT governance structure and require the use of reconstituted governance boards for all major IT decisions and investments. Further, we recommend revision of the board charters to include all information critical to ensuring the effective use of the boards and development of a plan to educate IT managers and personnel regarding the roles and responsibilities of the boards. Finally, in light of the changes recommended in this report, the NASA Administrator should reevaluate the resources of the OCIO to ensure that the Office has the appropriate number of personnel with the appropriate capabilities and skill sets.

In response to a draft of this report, NASA's Administrator concurred or partially concurred with our recommendations and proposed corrective actions to improve NASA's IT governance. We consider the Administrator's planned actions responsive and will close the recommendations upon verification that the Agency has completed them.

*** End of excerpt from the NASA audit report "NASA's IT Governance" ****

Case Questions

1. Read the full report at https://webmail.ontario.ca/owa/redir.aspx?C=U2esClUJnkSdZM8U7MibzLQDIdGY39AI9lLdeAxW11j_fFAJP8_6cj2ync6_Wh_Ym7-uXuUX9Mo.&URL=http%3a%2f%2foig.nasa.gov%2faudits%2freports%2fFY13%2fIG-13-015.pdf.

2. Research the NASA web site and learn about NASA from Google.

3. Write an IT strategy for NASA.

RUNNING CASE – Blackberry

We will use Blackberry as a running case throughout the book to apply the concepts from each chapter.

Background

As recent as 2008, many people thought that Research In Motion (RIM) would rule the world's mobile computing. It was trendy to check messages in elevators and restaurants with a Blackberry. Never before had I seen adults so agile with their thumbs. RIM common stock was traded at $140 a share, and it commanded more than 50% of the smart phone market share.

BlackBerry, which once dominated the smartphone market, has seen its market share drop to under 1 percent, as the iPhone and a slew of Android devices from Samsung have captured market share. John Chen, a turnaround expert brought in to fix its slide, is now pivoting BlackBerry to focus more on its well-regarded software and device management business.

Blackberry Limited, formerly known as Research In Motion Limited (RIM), is best known as the developer of the BlackBerry brand of smartphones and tablets. The company is headquartered in Waterloo, Ontario, Canada. It was founded by Mike Lazaridis, who served as its co-CEO along with Jim Balsillie until January 22, 2012, when the Board promoted Thorsten Heins as CEO. In January 2013, RIM changed its name to Blackberry. In November 2013, as the Company realized that the Blackberry 10 launch had not turned around its fortune and that the quarter ending that month will show a loss of over $4 billion, Heins was dismissed and replaced with John Chen, former CEO of Sybase (a software firm subsequently bought by SAP).

RIM's early development was financed by Canadian institutional and venture capital investors in 1995 through a private placement in the privately held company. Working Ventures Canadian Fund Inc. led the first venture round with a $5 million investment

with the proceeds being used to complete the development of RIM's two-way paging system hardware and software. A total of $30 million was raised by the company prior to its initial public offering on the Toronto Stock Exchange in January 1998 under the symbol RIM. Today (June 16, 2015), Blackberry is traded on Toronto Stock Exchange at $11.56 a share with a market value of just over $6 billion and net book value of $3.4 billion.

Product Development

In the late 1990's, RIM worked with RAM Mobile Data and Ericsson to turn the Ericsson-developed Mobitex wireless data network into a two-way paging and wireless email network . The pager was later improved to be a personal digital assistant capable of receiving messages sent between two Blackberries, email through email servers hosted by an Internet service provider and corporate email forwarded via Blackberry Enterprise Server installed in business organizations that allow employees to get email while on the road.

RIM soon began to introduce BlackBerry devices aimed towards the consumer market as well, beginning with Blackberry Pearl 8100 - the first BlackBerry phone to include multimedia features such as a camera. The introduction of the Pearl series was highly successful, as was the subsequent Curve 8300 series and Bold 9000. Extensive carrier partnerships fueled the rapid expansion of BlackBerry users globally in both enterprise and consumer markets.

The arrival of the first Apple iPhone in 2007 caused much fanfare and speculation that the BlackBerry might have its first serious competition. Boasting a powerful mobile browser, a new touch screen interface, strong multimedia capabilities and a bundled application storefront with many mobile apps, the iPhone was referred to as a "BlackBerry Killer" by some in the media. The introduction of iPhone on the AT&T network in the fall of 2007 in the United States prompted RIM to produce its first touchscreen smartphone for the competing Verizon network in 2008 - the Blackberry Storm. The Storm sold well but suffered from mixed to poor reviews and poor customer satisfaction. The iPhone initially lagged behind the BlackBerry in both shipments and active users, due to RIM's head start and larger carrier distribution network. In the United States, the BlackBerry user base peaked at approximately 21 million in the fall of 2010. That quarter, the company's global subscriber base stood at 36 million users. As the iPhone and Google Android accelerated growth in the United States, BlackBerry users began to turn to other smartphone platforms. Nonetheless, the BlackBerry line as a whole continued to enjoy success, spurned on by strong international growth. In October 2013, the company had 80 million BlackBerry users globally with about 9 million in the United States.

When the Apple iPhone was first introduced in 2007, it generated substantial media attention, with numerous media outlets calling it a "Blackberry Killer". The media attention to the iPhone drew consumer interest to smartphones in general, with both RIM

and Apple substantially increasing sales as the market itself grew substantially. In addition, both ate into sales of older competitors, such as Windows Mobile and Palm. While BlackBerry sales continued to grow, the newer iPhone grew at a faster rate.

The first three models of the iPhone lagged behind the Blackberry in sales, as RIM had major advantages in carrier and enterprise support, however Apple continued gaining market share. In October 2008, Apple briefly passed RIM in quarterly sales when they announced they had sold 6.9 million iPhones compared to 6.1 Blackberries sold. iPhone sales declined to 4.3 million units in the subsequent quarter and RIM's increased to almost 8 million units. This may have given RIM a false sense of security. Apple's iPhone began to sell more phones quarterly than the Blackberry in 2010, brought on by the release of the iPhone 4.

Following numerous attempts to upgrade its existing Java platform, RIM made numerous acquisitions to help it create a new, more powerful BlackBerry platform, centered around its acquired real time operating system QNX. In March 2011, Jim Balsillie suggested during a conference call that the "launch of some powerful new BlackBerrys" (eventually released as Blackberry 10) would be in early 2012.

On September 27, 2010, RIM announced the long-rumored Blackberry Playbook tablet, the first product running on the new QNX platform known as Blackberry Tablet OS. The BlackBerry Playbook was officially released to US and Canadian consumers on April 19, 2011, a year after Apple’s launch of iPad. The Playbook was criticized for being rushed to market in an incomplete state and sold poorly. Following the shipments of 900,000 tablets during its first three quarters on market, slow sales and inventory pileups prompted the company to reduce prices and to write down the inventory value by $485 million. Eventually, in October 2012, the highest end Playbook had a retail price as low as $150, which is what I paid. Compared to the high end first generation of iPad that I bought in April 2010 (for about $800), my Playbook is slower, has a small screen, and the touch screen is less sensitive.

Recent Development

In October 2011, RIM unveiled BBX, a new platform for future BlackBerry smartphones that would be based on the same QNX-based platform as the Playbook. However, due to an accusation of trademark infringement regarding the name BBX, the platform was renamed BlackBerry 10. The task proved to be daunting, with the company delaying the launch in December 2011 to some time in 2012. On January 22, 2012, Mike Lazaridis and Jim Balsillie resigned as the CEOs of the company, handing the reins over to executive Thorsten Heins. On March 29, 2012, the company reported its first net loss in years. Heins set out the task of restructuring the company, including announcing plans to lay off 5,000 employees, replacing numerous executives, and delaying the new QNX-based operating system for phones ("BlackBerry 10") a second time to January 2013.

After much criticism and numerous delays, RIM officially launched BlackBerry 10 and two new smartphones, Z10 and Q10, on January 30, 2013. The BlackBerry Z10, the first BlackBerry smartphone running BlackBerry 10, debuted worldwide in January 2013, going on sale immediately in the UK with other countries following. A marked departure

from previous BlackBerry phones, the Z10 featured a fully touch-based design, a dual-core processor, and a high-definition display. BlackBerry 10 had 70,000 applications available at launch, which the company expected would rise to 100,000 by the time the device made its debut in the United States. In support of the launch, the company aired its first Super Bowl television advertisement in the U.S. and Canada In discussing the decision to create a proprietary operating system instead of adopting an off-the-shelf platform such as Android, Heins noted, "If you look at other suppliers' ability to differentiate, there's very little wiggle room. We looked at it seriously—but if you understand what the promise of BlackBerry is to its user base it's all about getting stuff done. Games, media, we have to be good at it but we have to support those guys who are ahead of the game. Very little time to consume and enjoy content—if you stay true to that purpose you have to build on that basis. And if we want to serve that segment we can't do it on a me-too approach." Chief Operating Officer Kristian Tear remarked "We want to regain our position as the number one in the world", while Chief Marketing Officer Frank Boulben proclaimed "It could be the greatest comeback in tech history. The carriers are behind us. They don't want a duopoly". Apparently, the Company bet its farm on Blackberry 10.

Blackberry has in recent years declined precipitously, in part because of intense competition from iPhone and Android brands. By October 2013, Blackberry's U. S. market share had fallen below 1% and its world wide market share was down to 1.5%, lagging way behind iPhone, Android and Windows. It is now considered by many, especially young people, to be "irrelevant". Blackberry has stronger representation in Europe but virtually no presence in China.

On October 10, 2011, RIM experienced one of the worst service outages in the company's history. Tens of millions of BlackBerry users in Europe, the Middle East, Africa, and North America were unable to receive or send emails and BBM messages through their phones. The outage was caused as a result of a core switch failure, "A transition to a back-up switch did not function as tested, causing a large backlog of data, RIM said." Service was restored Thursday October 13, with RIM announcing a $100 package of free premium apps for users and enterprise support extensions.

On September 20, 2013, the company announced it would lay off 4,500 staff, and take a $1billion operating loss. Three days later, the company announced that it had signed a letter of Intent to be acquired by a consortium led by Prem Watsa owned Fairfax Financial Holdings for a $9 per share deal. However the company would remain open to alternative offers till November 4, 2013. On that day, Watsa's group announced that it would finance $1billion in convertible debenture instead of taking over the Blackberry, and installed John Chen as CEO to replace Heins.

In December 2013, the Company released its Q3 earnings which disclosed a $4.4 billion quarterly loss largely made up of inventory write down, or $8.37 per share. John Chen announced more layoff.

On the day of the earning release, Blackberry announced a 5-year partnership with Foxconn, the principal assembler of iPhone, to design and manufacture on a profit-sharing and just-in-time inventory basis. The stock market reacted favorably to this news as it would avoid significant inventory writedown. The initial focus of the partnership will be a smartphone for Indonesia and other fast-growing markets targeting early 2014.

"This partnership demonstrates BlackBerry's commitment to the device market for the long-term and our determination to remain the innovation leader in secure end-to-end mobile solutions," said John Chen, Executive Chair and CEO of BlackBerry. "Partnering with Foxconn allows BlackBerry to focus on what we do best - iconic design, world-class security, software development and enterprise mobility management - while simultaneously addressing fast-growing markets leveraging Foxconn's scale and efficiency that will allow us to compete more effectively."

Under the partnership, Foxconn will manufacture products for BlackBerry at facilities in Indonesia and Mexico. BlackBerry will own all of its intellectual property and perform product assurance on devices through the Foxconn partnership, as it does currently with all third-party manufacturers.

"BlackBerry is an iconic brand with great technology and a loyal international fan base," said Terry Gou, Founder and Chairman, Foxconn. "We are pleased to be working with BlackBerry as it positions itself for future growth and we look forward to a successful strategic partnership in which Foxconn will jointly develop and manufacture new BlackBerry devices in both Indonesia and Mexico for new and existing markets." Gou, a disciplined and aggressive CEO, has stated that Foxconn will design new Blackberry phones and showcase them in Mobile World Congress in February 2014, a show which Mark Zuckerberg will attend. One of the new features in the phones will be data-free FM radio, which iPhones don’t have, and Samsung phones once had but later was discontinued by Samsung.

On January 21, 2014, the Company announced that it would sell most real estate in Canada and lease back the necessary space for its operation. The market also reacted favorably. It is estimated the Company will generate $300 million in cash from selling the properties.

On February 14, 2014, U. S. hedge fund Third Point LLC announced having bought 2% stake of Blackberry in the open market.

In June 2014, Blackberry announced the following:

- Launching of BBM Protected using per message encryption keys compatible with United States Federal Information Processing Standard for cryptography.
- Plan to develop a phablet.
- Launching of Blackberry 10.3 in the fall which will accommodate Amazon apps, to augment the current 130,000 Blackberry apps. This will allow users to download popular Amazon apps like Netflix and Groupon. Blackberry stock rose 4% following this announcement.

On July 29, 2014, Blackberry announced the acquisition of Secusmart, a German developer of mobile encryption and anti-eavesdropping tech, subject to regulatory approval. Terms are undisclosed. The purchase comes amid an uproar in Germany over the alleged United States National Security Agency (NSA) spying activity, one that has even led Germany's NSA inquiry chief to suggest using typewriters to avoid eavesdropping. The German government was reported to be interested in buying 20,000 more Blackberry 10 phones for security reasons.

On November 13, 2014, BlackBerry announced it was partnering with Samsung to create an end-to-end security offering for Samsung's Android hardware; it features BES12 and Samsung's KNOX enterprise security platform. As part of the deal, Samsung will begin reselling BES12 in early 2015. Blackberry stock price rose 7% after the announcement. Critics however, doubt that this will significantly help the bottom line.

On June 11, 2015, Reuters reported that BlackBerry was considering a move to test run Android on its upcoming slider device, as part of a bid to convince potential corporate and government clients that its device management system, BES12, is truly able to manage and secure not just BlackBerry devices, but also devices powered by Google's Android, Apple's iOS and Microsoft's Windows operating system.

Leadership Changes

The company was often criticized for its dual CEO structure. Under the original organization, Mike Lazaridis oversaw technical functions, while Jim Balsille looked after the sales and marketing functions. Some saw this arrangement as a dysfunctional management structure and believed RIM acted as two companies, slowing the effort to release the new BlackBerry 10 operating system.

On January 22, 2012, RIM announced that its CEOs Balsillie and Lazaridis had stepped down from their positions. They were replaced by Thorsten Heins. Heins hired investment banks RBC Capital Markets and JP Morgan to seek out potential buyers interested in RIM, while also doubling efforts on releasing BlackBerry 10 (BB10).

On March 29, 2012, RIM announced a strategic review of its future business strategy that included a plan to refocus on the enterprise business and leverage on its leading position in the enterprise space. Heins noted, "We believe that BlackBerry cannot succeed if we tried to be everybody's darling and all things to all people. Therefore, we plan to build on our strength." Balsillie resigned from the board of directors in March 2012, while Lazaridis remained on the board as vice chairman.

Following the assumption of role as CEO, Heins made substantial changes to the company's leadership team. Changes included the departures of Chief Technology Officer David Yacht; Chief Operating Officer Jim Rowan; Senior Vice President of Software Alan Brenner; Chief Legal Officer Karima Bawa; and Chief Information Officer Robin Bienfait.

Heins hired Kristian Tear to assume the role of Chief Operating Officer, Frank Boulben to fill the Chief Marketing Officer role and appointed Dan Dodge, the CEO of QNX, to take over as Chief Technology Officer. On July 28, 2012, Steven E. Zipperstein from Verizon was appointed as Vice President and Chief Legal Officer.

On March 28, 2013, Lazaridis relinquished his position as vice chairman and announced his resignation from the board of directors. He is still a significant shareholder. Later in the year, Heins was replaced by John Chen, who was appointed Executive Chairman and CEO in November. Heins received an exit package of $22 million. Prior to joining BlackBerry, John Chen served as Executive Chairman and CEO of Sybase Inc., where he developed and led the company's re-invention from a mature, slower-growth technology company into a $1.5 billion-plus high-growth innovator. Under his direction, Sybase became the leading provider of enterprise mobility and mobile commerce solutions, achieving 55 consecutive quarters of profitability. Chen has been given a free hand by the Board to return Blackberry to profitability.

Kristian Tear and chief marketing officer Frank Boulben left in December 2013. Chief financial officer Brian Bidulka was replaced by James Yersh in December, who has been with the company since 2008, Board member Roger Martin, former Dean of Rotman School of Management of University of Toronto, resigned in late 2013. Tear was finally replaced by Marty Beard. Beard was most recently chief executive officer of LiveOps Inc, a provider of cloud applications for customer service. Prior to that he was an executive of Sybase.

New managing directors were appointed for the Africa and UK operations, shortly after Chen took the rein. Both are local staff members promoted to the jobs. Blackberry parted with Creative Director Alicia Keys on January 31, 2014. Alicia, a singer, was appointed to the job by Thorsten Heins a year earlier. Shortly after her appointment, she got into hot water by sending a Tweet from her iPhone.

In January 2014, Chen brought in Ron Louks, former chief technology officer of Sony Ericsson as President of Devices and Emerging Solutions. Earlier, John Sims was appointed as President, Global Enterprise Services, Blackberry.

Chen receives a $1 million annual salary and may be entitled to a performance bonus of $2 million annually. But his real chance to make big bucks comes in the form of 13 million restricted shares. If Chen actually rescues BlackBerry, these restricted shares could be worth a lot more. However, he will have to stick around for three years to get 25% of those shares, four years for the next 25% and five years for the remaining 50%. If Chen is terminated "without cause," which is often the case even when a CEO is essentially fired, he will continue to receive his $1 million annual salary through the remainder of the year in which he leaves the company. On top of that, he'll receive an extra award of two times his base salary and two times his bonus, for a total of $6 million more.

On February 10, 2014, Andrew Bocking, executive vice-president for BlackBerry Messenger, resigned. He oversaw the introduction of BBM to iPhone and Android devices in October. John Chen has singled out BBM as a pillar for growth. John Sims has taken on responsibility for the messaging service.

Other directors include:

Prem Watsa, Chairman of Fairfax Financial, which owns 10% of Blackberry.

Barbara Stymiest, Chair of the Blackberry board and former Group Executive of RBC Financial Services.

Timothy Dattels, former Partner and Managing Director of Goldman Sachs, with strong Asia Pacific connection.

Claudia Kotchka, Certified Public Accountant and independent consultant.

Richard Lynch, former chief technology officer of Verizon.

Michael Daniels, Chairman of Invincea, a venture backed provider of advanced cyber security technology solutions.

Workforce Reduction

In June 2011, RIM announced its prediction that Q1 2011 revenue would fall for the first time in nine years, and also unveiled plans to reduce its workforce.

In July 2011, the company cut 2,000 jobs, the biggest lay-off in its history and the first major layoff since November 12, 2002 when the company laid off 10% of its workforce (200 employees). The lay-off reduced the workforce by around 11%, from 19,000 employees to 17,000.

On June 28, 2012, the company announced a planned workforce reduction of 5,000 by the end of its fiscal 2013, as part of a $1 billion cost saving initiative.

On July 25, 2013, 250 employees from Blackberry's research and development department and new product testing were laid off. The layoffs were part of the turnaround efforts.

On September 20, 2013, Blackberry confirmed that the company would have a massive layoff of 4,500 more employees by the end of 2013. This would be approximately 40 percent of the company's workforce. In a letter to staff, John Chen said as the Company transitioned, no job is safe.

On August 1, 2014, BlackBerry announced that it had concluded a protracted and painful restructuring process and is back on a growth footing, according to an internal memo to all its employees viewed by Reuters. "We have completed the restructuring notification process, and the workforce reduction that began three years ago is now behind us," said the memo from BlackBerry's Chief Executive John Chen. "More importantly, barring any

unexpected downturns in the market, we will be adding headcount in certain areas such as product development, sales and customer service, beginning in modest numbers," said Chen, who personally thanked those that have stayed with the company through the process. BlackBerry has shrunk its workforce by roughly 60% over the last three years as it attempted to reinvent itself. He noted also BlackBerry, which had previously said it was trimming its workforce down to 7,000 from a peak of over 17,500 in 2011, is now in a position to make strategic acquisitions to strengthen areas that are likely to drive future revenue growth. Chen told employees that he is confident BlackBerry now has the right organization and team in place to execute its business strategy. Over the last few months, he has hired a number of former Sybase employees that helped engineer that turnaround before the company was sold to software giant SAP AG in 2010. Chen stressed in the memo there was "no margin for error to complete BlackBerry's turnaround to success", and he called on employees to remain focused as the company rolls out an upgrade to its device management system and release new phones.

Platform Transition

BlackBerry Operating System (Java)

The original Java-based Blackberry operating system (OS) was suitable for low powered devices, narrow network bandwidth and high security enterprises. However, as the needs of the mobile user evolved, the aging platform struggled with emerging trends like mobile web browsing, consumer applications, multimedia and touch screen interfaces. Users could experience performance issues, usability problems and instability.

The company tried to enhance the aging platform with a better web browser, faster performance, a bundled application store and various touch screen enhancements, but ultimately decided to build a new platform with QNX at its core. While most other operating systems are monolithic - the malfunction of one area would cause the whole system to crash – QNX is more stable because it uses independent building blocks or "kernels", preventing a domino effect if one kernel breaks. RIM's final major OS release before the release of Blackberry 10, was Blackberry 7, which was often criticized as dated and referred to as a temporary stopgap.

BlackBerry Tablet OS (QNX)

The Blackberry tablet was the first RIM product whose Blackberry Tablet OS was built on QNX, launched in April 2011 as an alternative to iPad. RIM named the tablet Playbook. However, it was criticized for having incomplete software and a poor application selection. It fared poorly until prices were substantially reduced, like most other tablet computers released that year. Blackberry Tablet OS received a major update in February 2012, as well as numerous minor updates.

BlackBerry 10 (QNX)

Blackberry 10, a substantially updated version of Blackberry Tablet OS, intended for the next generation BlackBerry smartphones, was originally planned for release in early 2012. The company delayed the product several times, remembering the criticism faced by the BlackBerry Playbook launch and citing the need for it to be perfect in order to stand a chance in the market. It reached the market in early 2013. Blackberry 10 has the following new features.

Multitasking - BlackBerry 10 OS supports multitasking with gesture integration. Swiping up from any application brings up the running application screen, which functions as an application switcher and a task manager. Users can switch through running applications by tapping on any of the apps or close them by tapping on the 'X' on the lower right of the app itself. In other words, unlike in an iPhone, a user does not have to go back to the menu to select a different application.

BlackBerry Hub – It acts as a notification center, with the user's entire social and email accounts integrated into one app. These include, at launch, standard email client, Twitter, Facebook, Blackberry Messenger (BBM), and LinkedIn. Standard notifications like missed calls, voicemail, and system updates also appear on the hub. The hub is accessible from any app/lock screen, by performing an upside down j-hook gesture. Users can perform various tasks like composing emails, sending emails, and browsing social networks, without accessing other apps. Developers are also given options to integrate apps into the Blackberry Hub.

BlackBerry Balance – Blackberry Balance is a new feature introduced in BlackBerry 10, enabling users to keep both personal data and office work data separated in its own spaces. Using Blackberry Enterprise Service 10, IT departments can allow users to set up work-spaces that automatically install applications and email accounts. After completion, users can navigate between personal and work profiles, by swiping down on the apps page. All of the user's data is secured via 256-bit encryption, and any files created will stay within the profile partition. At launch, some corporate clients that did not want to avail the personal work space to employees found it unable to deactivate that half. A fix was soon released to do that.

Time Shift Camera - BlackBerry 10 features camera software that takes multiple frames of every photo. This feature allows users to adjust a photo easily to correct issues such as closed eyes.

Blackberry Video/Screen Share - BBM in BB10 includes the ability to video chat and make VOIP calls as well as the ability to share the content of a user's screen with others for free on wifi or on your mobile data plan.

Intelligent keyboard – The OS is able to guess what your next keystrokes are based on a few letters which you an accept or edit.

Products

Blackberry's main hardware product is the Blackberry series of smart phones running on Blackberry 7 and Blackberry 10. Blackberry 10 sales are slow. More than 74% of the phones sold is Q3 of fiscal 2014 were Blackberry 7. Corporate customers can purchase these handsets from Blackberry or through a phone carrier. Consumers can only go through a phone carrier. John Chen wants to keep the physical keyboard on Blackberry handsets and in fact wants to focus on producing phones with the keyboard, as he thinks that's what corporate customers want and it differentiates Blackberry from competitors. Playbook is no longer supported.

The main messaging products are Blackberry Internet Service (BIS), Blackberry Messenger (BBM) and Blackberry Enterprise Server (BES). BIS allows users to access web mail. BBM facilitates exchange of short messages up to 2,000 characters, voice notes and videos; users can also make video calls. BES is used by corporate clients to forward their email to employees' handsets. BES is also available for licensing for use on iPhones and Android devices. In addition, QNX is used in automobiles for computer control and this product is marketed and supported by Blackberry's QNX subsidiary. Blackberry World is the online stores that allow registered users to buy apps and download free apps.

Blackberry 10 Phone

The following Blackberry phones run on Blackberry 10:

Passport – This square phone comes with an alphabetical physical keyboard and also a touch screen keyboard. It has 3 gig in RAM and 32 gig flash memory upgradable to 64 gig, 13 meg rear camera, 2 meg front camera. It features a 4.5 inch display. This phone is targeted to business users who will find it easy to read text like documents. This phone, launched in September 2014, will carry an unsubsidized price of $599. Blackberry stock rose by 1% on the launch day. The keyboard is easy to use, with bigger and flatter keys than those in older Blackberry phones.

Z30 - The BlackBerry Z30 is a high-end 4G touchscreen phone. Announced on September 18, 2013, it succeeded the Z10 as the first totally-touchscreen device to run the Blackberry 10.2 operating system. The Z30 includes a 5-inch display, 2 gig RAM, 16 gig flash memory expanded to 64 gig, 8 meg rear camera, 2 meg front camera. It features a 5 inch screen.

Q10 – This is the first physical keyboard phone running on Blackberry 10. There are also touchscreen functions. It is a 4G phone that features a 3.1 inch display, Everything else is essentially the same as the Z30.

Q5 is the third Blackberry 10 phone designed for emerging markets. It is also a 4G phone. The built-in memory has 8 gig which is expandable to 32 gig. The rear facing camera has 5 meg. Everything else is essentially the same as the Q10.

Blackberry phones are equipped with a near field communication (NFC) chip that enables the phones to be used for banking and payments like a debit or credit card. Canadian banks are adapting to this technology. NFC permits contactless transfer of information within four centimeters.

All Blackberry 10 phones can run Android apps. They can also run iOS apps with an iOS Player, less seamless than running Android apps.

Blackberry announced in June 2014 that a new phone, named Passport, would be released in September in the U. K. It will be a square device with larger physical keys and a 4.5 inch display that is 3.18 inch wide. This business oriented phone is designed for spreadsheet lovers and PDF readers. Rumored to run a 2.5GHz quad-core Snapdragon 801 processor and 3GB of RAM, the Passport will also be bestowed with an 8-megapixel rear-mounted camera and a secondary 3.7-inch snapper up front.

Blackberry Internet Service

BlackBerry Internet Service (BIS) is an email and synchronization service for BlackBerry users. BIS was created for BlackBerry users without an enterprise email account on a BlackBerry Enterprise Server (BES). BIS allows you to retrieve email from web mail or Outlook Web App (OWA) on your BlackBerry, and synchronize your contacts, calendar, and deleted items from some email providers. OWA is web access to corporate Outlook email. You can also set up a Blackberry.net email account through your wireless carrier and access it with BIS.

Blackberry Messenger

Blackberry Messenger (BBM) is a handset to handset messaging system. It also allows online chat in groups. It is popular among young people and users in South East Asia. Recently, BlackBerry has enabled the messenger (BBM) to be active on non-BlackBerry devices. Within 60 days of its launch, the app saw more than 40 million new iOS and

Android users registering to use it. Blackberry 10 supports video calls using BBM. There are 70 million BBM users worldwide. All BBM messages go through the Blackberry infrastructure hosted by Blackberry. Here is a list of common features.

- Make BBM Video calls using Blackberry 10, like iPhone’s Facetime.
- Send and receive messages across platforms, using your data plan or wifi.
- Choose a personal BBM display picture and status.
- Real-time confirmations when messages are being written, delivered and read.

- Share photos, videos and more with multiple contacts at once. Each file must not be more than 6 megabytes. Video sharing is only available to Blackberry 10 clients.
- Add contacts by scanning Quick Response (QR) Codes, using near field communication (NFC) technology or sharing Personal Identification Numbers (PIN).
- Send music files.
- Create and join groups where you can share and discuss lists, photos etc.
- Share location.

Exchanging messages is possible to a single person or via dedicated discussion or chat groups, which allow multiple BlackBerry devices to communicate in a single session. In addition to offering text-based instant messages, BlackBerry Messenger also allows users to send pictures, voicenotes (audio recordings), files, location on a map and a wide selection of emoticons. Users can even make videocalls. BBM messages are compressed in transmission so they are more economical than texting and Blackberry Internet Service email (web mail). They also use less bandwidth than emails.

Messages can be transmitted to the recipients based on their PINs or email addresses. The 8-character PIN is randomly generated by Blackberry upon BBM enrolment and bears no textual correlation to the user's other identities. It is controlled by the user in terms of how and who to share the PIN. Before given a PIN, a user has to obtain a BBID from Blackberry. The BBID is the user's account ID with Blackberry for BBM and is not transmitted in messaging.

With the release of BlackBerry Messenger 5.0, BlackBerry allows users to use a QR code to add each other to their respective friends lists rather than using only alphanumeric PIN identification or an email address associated with the user's BlackBerry.

Recent BlackBerry devices can also exchange BBM contacts using NFC technology. NFC is really just a short range radio frequency ID. This means two phones within four centimeters can exchange contacts, in a way, a touchless handshake.

A BBM message and attached files are sent from the handset to the wireless carrier, then to a Blackberry network operations center (NOC), then to the recipient's wireless carrier, then to the recipient. BBM is free but the service makes Blackberry handsets more attractive and make carriers more likely to stock and sell Blackberry phones.

Blackberry Enterprise Server

This is now Blackberry's crown jewel, the only profitable product. It is what keeps large organizations in Blackberry's clientele. Organizations that want to forward their corporate email to employees can license Blackberry Enterprise Server (BES) and installs it on local servers. Email from the corporate mail server is then forwarded to a BES

server within the organization, then to the organization's Internet service provider (ISP), then to a Blackberry NOC, then to the organization's wireless carrier, then to the handset. BES mail sent from a handset travels in reverse direction, then out to recipient via the organization's ISP.

Depending on the email system being used, the mechanism used to figure out what has changed is different. In an Exchange environment, BES makes a request to the Exchange server and asks that it be told whenever a new email arrives. The Exchange server duly obeys and when a new email arrives it notifies the BES, which in turn grabs a copy of that new email and sends it to the BlackBerry. Forwarded emails are stored in the handsets subject to truncation of long content so they can be read offline. Users can compose replies offline which will be sent once the unit is online. BES messages are compressed during transmission and hence travel faster than email messages going to other phone brands and for the same reason keep the battery lasting longer before having to be recharged.

As a BES user you can:

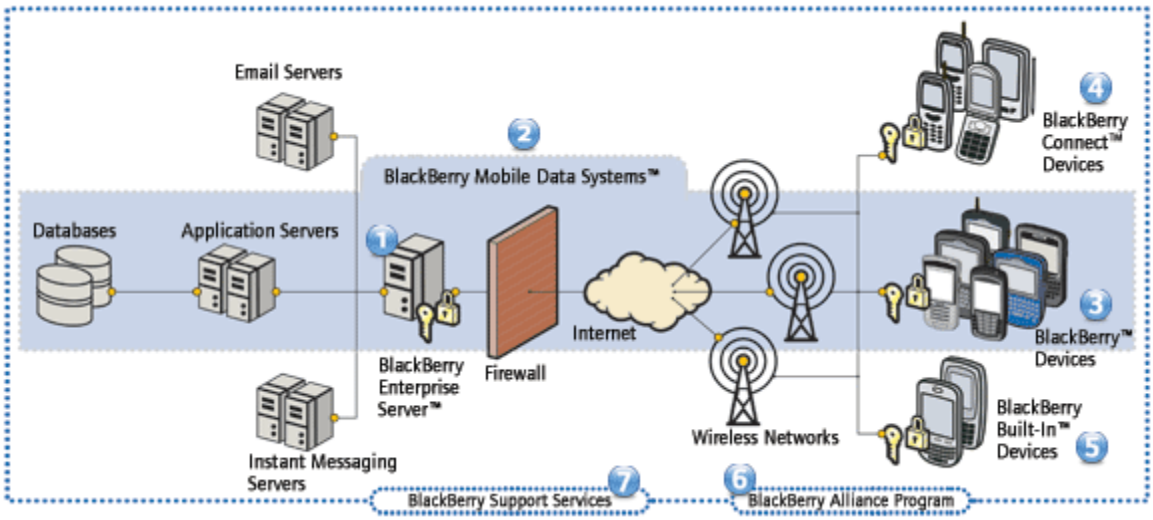
- Receive email in real time.
- Have a message that you read on your BlackBerry show up as read back in your corporate inbox (and vice versa) automatically.
- Move a message to an existing folder within your corporate inbox from your BlackBerry.
- Have a message that you delete on your BlackBerry be moved to the Trash folder in your corporate inbox automatically.
- Have your corporate address book bi-directionally synchronized wirelessly with your BlackBerry.
- Have your corporate calendar bi-directionally synchronized wirelessly with your BlackBerry.
- Set up meetings from your BlackBerry, invite attendees, and see their free/busy status.
- Look people up in the company global address book when composing new email in real time.
- Set up or change your Out Of Office message and enable or disable it.
- Browse the internal company web sites.
- View or download email attachments.

On November 13, 2014, BlackBerry launched BES12. The latest version of BlackBerry's mobile device/app management platform supports up to 25,000 devices per server and 150,000 devices for each domain. It features a revamped endpoint management model said to enable "more flexible management of devices, applications and data."

Blackberry Network Operation Center (NOC)

The NOC is a key part of the BlackBerry BES solution. When a BES is first installed it is assigned a unique address called a Server Relay Protocol (SRP) ID or number. This SRP ID uniquely identifies the BES and in fact no two BESs can use the same SRP ID.

When the BES starts up, it actually logs into a NOC using its unique SRP ID or address. The NOC accepts the login if the SRP address is valid, and becomes aware of the BES. Any BlackBerry that has been activated on a BES will have the SRP ID or address. When the BlackBerry itself is turned on, it registers with the NOC using its PIN number. Now the NOC is aware of the BlackBerry and the BES. This allows the BlackBerry and BES to communicate with one another via the NOC. The following diagram copied from Crackberry.com, a web site hosted by devoted Blackberry users, shows how BES and corporate supported BBM messages travel.



The NOC is not shown, however it sits between the wireless networks and the Internet. It is the point where BlackBerry and BES can find each other and communicate. The NOC takes care of handling individual BlackBerry connections and also queues up data that is destined for a BlackBerry when it is out of coverage or turned off. This means that the BES itself doesn't need to worry about doing that extra work. Blackberry NOCs are in North America, England and India.

BES differs from iOS, Android and Windows phones in that the latter do not route messages through a NOC. Instead, messages go from handset to wireless carrier, to Internet service provider (if the message is an email to be forwarded via a desktop oriented email system like Exchange or Gmail), then to wireless carrier of the recipient and to the recipient handset. Some see a NOC as a single point of failure even with redundancy. This worry materialized in late 2011 when the UK NOC went down

QNX

QNX is a commercial, Unix like operating system aimed primarily at the embedded systems market. The product was originally developed in the early 1980s by Canadian company Quantum Software Systems, later renamed QNX Operating Systems and ultimately acquired by RIM in 2010 for $200 million, five times the annual revenue. QNX was one of the first commercially successful microkernel operating systems and is used in a variety of devices including the world's highest capacity Internet routers, flight simulators, air traffic control, shipping navigation systems, high speed train controllers, in-car information, entertainment and control systems, warehouse distribution systems, cable TV delivery, Hollywood special effects systems, smartphones, mobile devices, casino gaming system as well as hospital and laboratory technology.

As a microkernel-based OS, QNX is based on the idea of running most of the OS in the form of a number of small tasks, known as *servers*. This differs from the more traditional monolithic kernel, in which the operating system is a single very large program composed of a huge number of "parts" with special abilities. The system is quite small, with earlier versions fitting on a single floppy disk. The kernel is a computer program that manages input/output requests from software and translates them into data processing instructions for the central processing unit and other electronic components of a computer. The kernel is a fundamental part of a modern computer's operating system. When a computer program (in this case called a *process*) makes requests of the kernel, the request is called a system call. Various kernel designs differ in how they manage system calls (time-sharing) and resources. For example, a monolithic kernel executes all the operating system instructions in the same address space to improve the performance of the system. A microkernel runs most of the operating system's background process in user space, to make the operating system more modular and, therefore, easier to maintain.

QNX Neutrino is widely used as the basis for automotive electromechanical components, for industrial control systems, medical instruments, defense systems, nuclear power plants, and other mission-critical applications.

Despite its wide use, QNX does not contribute significantly to Blackberry’s bottom line. This is because QNX is only a small part, albeit an essential part, of embedded systems that use it. It is not a ready-to-deploy operating system for end users like Windows or iOS. This is why it took two years for Blackberry to build Blackberry 10. Blackberry will have to be innovative from a marketing and product development perspective to monetize QNX.

The most recent good news about QNX is that Ford announced in February 2014 that it was dumping Windows in favor of QNX for its Sync system. QNX is be faster, cheaper and more flexible. Sync, which is in over 7 million vehicles, allows drivers to make mobile-phone calls and play music using voice-activation. Getting Sync right appears to be rather important - surveys indicate that in-vehicle technology is the leading selling point for 39% of auto buyers.

Here are some other QNX applications:

1. Apple's CarPlay runs on it.
2. Caterpillar's mining division uses QNX in surface mine control systems.
3. QNX Neutrino RTOS powers most Cisco products.
4. Emerson employs QNX in systems used to manage the operation of oil refineries and food manufacturing.
5. General Electric uses QNX for precision timing and applies it to steam turbine controls, and large turbine control systems.
6. The US Postal System uses QNX to run the delivery barcode system and sort 35,000 to 40,000 letters per hour.
7. The US Army, NASA, Boeing, and Lockheed Martin use QNX on mission-critical systems. Unmanned aircraft control systems, autonomous underwater vehicles, guidance systems for anti-tank weapons, and wearable GPS for ground troops all contain QNX.

Competition

Blackberry's handsets continue to be under stiff competition. Despite periodic press releases about new features and many analysts' opinion that the hardware is sturdy, it seems to lack the "cool" factor that appeals to young or affluent users. When Apple released its Q1 result in January 2014, it indicated that sales of the more expensive iPhone 5S exceeded that of a less powerful iPhone 5C. Apple thought the iPhone 5C would outsell iPhone 5S. This shows that iPhone fans are willing to pay more for a premium Apple product whereas Blackberry has had trouble attracting that kind of following. Some people say that using a Blackberry gets you reliability but using an iPhone or Samsung Galaxy gives you reliability and fun. Blackberry management has given up competing with Apple and Samsung on the consumers front and will focus on corporate users. This is one of the reasons Blackberry indicated that it would make phones primarily with a physical keyboard to keep its legacy and appeal to mature and business users. Outsourcing the design and assembly of handsets to Foxconn further shows that Blackberry wants to devote its effort and resources to software and network security instead of pursuing seemingly winless battles on the hardware front.

Even on the network and security platforms, the path to retaining its corporate user loyalty is tough. Apple and Samsung are aggressively targeting the corporate market. For many corporate users, it seems to be just as easy to access corporate email using other smart phones. Blackberry will have to reassess the value BES and BBM, especially in terms of the cost of routing all messages through a NOC and passing the cost to customers. To survive, the Company has to look beyond keeping BES, BBM and

Blackberry 10 phones in their present forms. The QNX value has to be unlocked to enter new fields. Blackberry has to design more innovative functions in security software, mobile devices and mobile data management.

With licensing of BES to organizations that use iOS and Android platforms, those organizations will be more inclined to stick with non-Blackberry phones. Also, organizations that do not mind going through the extra steps of using Exchange Active Syn to simulate the BES features will not even license BES. Exchange ActiveSyn allows organizations to push email to handsets with encryption.

Blackberry has stated that its consumer business will be focused on emerging markets. It wants to main it dominance in Indonesia. However, competition will come quickly from inexpensive Chinese brands like Huawei, which is priced at retail as low as $100 without a contract.

On July 15, 2014, IBM announced an alliance with Apple to sell iPhones and iPads to its business clients loaded with business applications.

Security

Blackberry announced on August 8, 2013 that its BlackBerry 10 phones, including the touch-screen Z10 and the keyboard-enabled Q10, in conjunction with its mobile device management (MDM) service BlackBerry Enterprise Service (BES) 10, have been awarded an "authority to operate," the highest level of certification on U.S. Defense Department networks. BES 10 was the first MDM solution for BlackBerry 10 on the market to receive such certification, the company said.

Receiving the authority to operate is an important step for the overall certification process in order to get BlackBerry smartphones running on U.S. government and military networks. The award is in effect a governmental rubber-stamp to the level of security the service provides.

A BlackBerry spokesperson said: "DoD users can fully embrace all of the consumer features – applications, games, multimedia, social networking — while still having full access to their DoD email."

DOD has also approved military use of iPhones and Android phones.

BES mail is encrypted with the Triple Digital Encryption Standard (DES) or Advanced Encryption Standard (AES) algorithm. These algorithms use symmetric keys, i.e., the same key is used to encrypt and decrypt. A different symmetric key is assigned to each Blackberry by the BES server.

Blackberry Messenger (BBM) emails are encrypted using a common key controlled by Blackberry for all Blackberry devices and are therefore less secure than BES emails. A user organization may choose to assign its own common BBM symmetric key for the

organization, for BBM emails within the organization, which, effectively, is more secure than relying on the common BBM encryption key. However, internally encrypted BBM email is much less secure than BES email.

On June 16, 2014, Blackberry announced the release of BBM Protected, which encrypts each message with a different key. The message symmetric key is encrypted with a static symmetric key exchanged once only between two parties the first time they contact each other using BBM Protected. This meets the United States Federal Information Processing Standards for cryptography.

Blackberry Internet Service does not have encryption by default. Blackberry has stated the following in its Knowledge Base.
Email messages sent between the BlackBerry Internet Service and the BlackBerry Internet Service subscriber's BlackBerry smartphone are not encrypted. When transmitted over the wireless network, the email messages are subject to the existing or available network security model(s).

"Existing or available network security models" above refers generally to Secure Socket Layer (SSL) encryption that is equivalent to eBusiness encryption at the option of the content or Outlook Web Access web site.
Other smart phones can also be connected to corporate email systems using other software such as Microsoft Exchange Active Sync, but encryption may be less consistently applied because the exchange server or user PC connected to the smart phone may not enforce encryption.

Here is a list of the Blackberry 10 security features:

- Transmission between BES server and Internet service provider (ISP) is encrypted using Transport Layer Security (TLS) or Secure Socket Layer (SSL), which uses eBusiness graded symmetric 128-bit keys.
- BES transmission from the ISP to a Blackberry NOC is encrypted using an AES key specific to each BES server.
- Transmission between a Blackberry NOC and a wireless carrier is encrypted using TLS or SSL.
- Transmission between a wireless carrier and the handset is encrypted using AES.
- Wifi can be encrypted using the required method specified by the access point (wireless router).
- TLS and SSL encryption can be enabled on the handset to secure web mail, OWA and eBusiness.
- Remote device killing, pushing of system configuration and purging of data.
- Forced password.
- Allowing limited apps in the work partition and personal partition.
- Malware protection.

On August 6, 2014, BlackBerry said its Android and iOS device-management service has won a key security clearance from the U.S. Defense Information Systems Agency (DISA). The Company said the DISA clearance will allow its customers in various U.S. Department of Defense agencies to begin to use its BlackBerry Enterprise Service (BES) 10 system to manage and secure devices powered by Google Inc's Android operating system and Apple Inc's iOS software. BlackBerry launched the service to manage rival devices on its BES system a year ago, as part of a move to help it sell high-margin services to its large clients even if many, or all, their workers use smartphones made by competitors. The new feature, dubbed Secure Work Space, is managed through BES 10, a new back-end system launched at the start of 2013 that allows BlackBerry's clients to control mobile devices on their internal networks. The decision to service non-BlackBerry devices is part of the company's move to reinvent itself as its own devices have waned in popularity.

Financial Condition

Blackberry's revenue comes mainly from handset sales and Blackberry Enterprise Server licenses. It expenses mainly include cost of sales for handsets, development cost and the cost of BES and BBM infrastructure in its NOCs.

Revenue from continuing operations for the fiscal year ended March 1, 2014 was $6.8 billion, down 38% from $11.1 billion in fiscal 2013. The Company's GAAP net loss from continuing operations for fiscal 2014 was $5.9 billion, or $11.18 per share diluted, compared with GAAP net loss from continuing operations of $628 million, or $1.20 per share diluted in fiscal 2013. Adjusted net loss from continuing operations for fiscal 2014 was $711 million, or $1.35 per share diluted. Cash burn rate from operation in the last fiscal year was significantly offset by sale of fixed assets.

Blackberry is in its worst financial stress since going public. The Company thinks it will return to profit in two years. Current assets sit at $5.1 billion including $2.5 billion in cash. Accounts payable net of receivables amounted to $564 million. Net fixed assets of $942 million (compared to 2.1 billion a year ago) are mainly in real estate and NOC infrastructure. Its patents are recorded in the books at about $1.4 billion (compared to $3.4 billion a year ago). The following table compares the Company's financial condition between the last two fiscal years. Amounts, except book value per share, are in US millions.

	February 28, 2015	**March 1, 2014**
Cash	$ 2,891	$ 2,529
Current assets	4,167	4,848
Intangibles	1,451	1,439
Total assets	6,549	7,552
Current liabilities	1,363	2,268
Total liabilities	3,118	3,927
Shareholders' equity	3,431	3,625
Revenue	3,373	6,792
Net loss per share	0.58	11.18
Book value per share	6.49	6.99

Questions

1. What do you think are Blackberry's business critical systems and why?
2. How technology savvy are Blackberry's board of directors and how important is that to the Company's success?
3. What are the technology risks of Blackberry?

MULTIPLE CHOICE QUESTIONS

1. Which system component affects a system's importance the most?

   A. Infrastructure
   B. Information
   C. Software
   D. People
   E. Procedures

2. Who is responsible for ensuring system reliability?

   A. Management
   B. Auditors
   C. CIO
   D. Chief risk officer

3. What should be a CEO's main concern about the annual doubling of computing power?

   A. Increasing spending
   B. Impact on audit fee
   C. Inappropriate use by employees
   D. Opportunity and risk

4. What affects an IT strategy the most?

   A. Annual doubling of computing power
   B. Regulatory requirement
   C. Business strategy
   D. Systems development plan

5. Which type of system has benefited the most from fast growth in computing power?

   A. Customer relationship management
   B. ATM
   C. Payroll
   D. Local area network

6. Who should own the customer relationship management system in a major Canadian bank?

   A. Chief financial officer
   B. Chief executive officer
   C. Head of personal banking
   D. Chief information officer

7. Which system component is most critical to ensure system availability?
    A. Information
    B. Infrastructure
    C. People
    D. Software
    E. Procedures

8. Which reliability concern is increased in cloud computing?
    A. Completeness
    B. Accuracy
    C. Timeliness
    D. Authorization

9. Which is the most relevant pair?
    A. Quantum computing and big data
    B. System owner and infrastructure
    C. Privacy and accuracy
    D. Peyton Manning and Roger Federer

10. Which position requires the most powerful system access?
    A. Chief information officer
    B. System owner
    C. System administrator
    D. Chief technology officer

CHAPTER TWO – INFORMATION AND INFORMATION TECHNOLOGY RISKS

"There are risks and costs to a program of action, but they are far less than the long-range risks and costs of comfortable inaction." – John F. Kennedy

- In January 2014, Target warned its Canadian customers that a massive security breach at the retailer over the holiday season might have led to their personal information being stolen. An email sent to some customers by the retailer said it believed cross-border shoppers who went to U.S. Target stores between Nov. 27 and Dec. 15 had been affected.
- In December 2013, Delta Airline's reservation system had a glitch for half a day that let customers book flights with huge accidental saving like business class flights from continental United States to Hawaii at 10% of the normal fare.
- In June 2012, LinkedIn investigated the possible leak of several million of its users' passwords after a member of a Russian online forum said he had managed to hack the popular networking site and upload close to 6.5 million passwords to the Internet.
- BlackBerry services returned to normal on October 13, 2011 after four days of global outage. In a conference call on October 13, Research In Motion explained that the widespread outage was caused by technical glitches linked to a backup switch that did not function as tested, causing a large backlog of emails and texts. Outage started in Europe, then spread to the Middle East, Africa and hit Canada on October 13. Parts of South America, as well as Asian markets were also affected.
- In March 2010, hackers flooded the Internet with virus-tainted spam that targeted Facebook's estimated 400 million users in an effort to steal banking passwords and gather other sensitive information.

In the last chapter, we talked about the need to assess inherent risks before developing and implementing internal controls in order to mitigate risks to an acceptable level and therefore provide an acceptable level of assurance on information system reliability. In this chapter, we will discuss the process of risk assessment. We will address risks from the standpoints of management and auditors.

A lot about risk management is common sense. We manage risk when we walk and drink coffee (a little sip first to see if it is too hot). We turn on the television to check the weather before leaving for work or university.

Computers are fast but mistakes can also multiply fast. Here is an example:

Lenovo Canada offered discounts to customers Tuesday after thousands were outraged when their orders were abruptly cancelled by the company over a "pricing error." During a "Door Buster" sale on its website on May 23, 2014, Lenovo Canada advertised its top of the line Y410P laptop on sale for just $279 that normally sells for close to $1,000. Soon after, customers began receiving emails from the company telling them their orders were cancelled.

Lenovo Canada responded to Global News' requests for comment on the issue on May 27. The statement reads in full:

"Between May 22 and May 23, 2014, a pricing error occurred on the Lenovo Canada website for select Lenovo laptops. The error mistakenly allowed a "doorbuster" e-coupon to be combined with an instant savings discount price. As a result, prices and the automatically generated calculation of discount percentages and savings appeared in error.

Once the error was discovered, Lenovo took steps to correct it. The prices on the Lenovo Canada website now reflect the correct price and price reduction. However, before we were able to correct the error, customers placed orders at the incorrect prices. As stated on our website and in the terms and conditions which customers agree to when purchasing a Lenovo product, Lenovo – like other computer manufacturers – reserves the right to cancel any orders for products placed at an incorrect price due to an error in pricing. We have informed the affected customers of the pricing error and we are in the process of cancelling their orders and any charges that occurred. We deeply regret any inconvenience this error has caused.

As a gesture of goodwill, starting May 28th, we will be contacting customers whose orders were canceled with an offer of $100 off their next purchase of a Lenovo laptop PC. This $100 can be deducted from the total order amount regardless of any discounts already applied to that order through August 3, 2014."

After Global News tweeted news of the statement, Lenovo customers reacted with anger on Twitter specifically regarding the offer of a coupon. Many customers said the offer was not good enough and felt the company should honor the sale price of the laptop.

Computers can be consistently right but also consistently wrong. Increasing use of information technology (IT) means less paper trail. The reduction in hard copy documents may render mistakes and irregularities more difficult to detect. The concentration of information in computers and electronic media exposes organizations to the risk of "placing all the eggs in one basket". Further, it is more difficult to control who has access. These are some basic risks in using IT. Other less obvious risks include improper use, uneconomical deployment, inadequate capacity and systems that do not meet business requirements.

There are basically three types of things that can go wrong with respect to using IT. First, the wrong system may be developed in relation to business requirements, the development of a system may not be well managed and therefore wasting the organization's money, or the system may be developed with significant flaws. Secondly, undesirable things might happen to a system when it is being used; e.g., unauthorized data changes may be made, there may be unauthorized use, disasters can happen that damage the hardware and software. Thirdly, system information may be inappropriately used; e.g., users are not trained and therefore misuse some functions, or there may be incorrect interpretation of system information. We will talk about the risk of inappropriate systems development in Chapter Four. The rest of this chapter will focus on the other two types of unfavorable system occurrences, the degree of which depends on the nature of business, organization and system.

The risk of errors or irregularities because of the nature of the business, organization and system is called inherent risk. An organization can avoid or reduce inherent risk by engaging in less ambitious business strategy, e.g., by abstaining from eBusiness. To mitigate such risk, management must implement internal controls. However, internal controls are not fool-proof otherwise they would be too expensive. The risk of internal controls not preventing or detecting significant errors is called control risk. The third definition of risk, to an auditor, is the risk of audit procedures failing to detect material errors, and this is called detection risk. Auditors are concerned about all three types of risk. The multiplicative value of inherent risk, control risk and detection risk is called audit risk, which is the risk of providing favorable audit assurance on a system which has a major flaw. Management is generally concerned about only inherent risk and control risk. The product of inherent risk and control risk is called “residual risk”, i.e., the risk remaining even after implementing internal controls. Management has to assess whether the residual risk is acceptable and organizations should have guidelines and decision limits to ensure consistent application and acceptance of residual risk. The tolerable residual risk should be low for every business critical system.

The term “threat” is often used to refer to risk. A threat is more general and it usually does not bear any quantifiable connotation. For example, a snow storm is a threat. The estimated likelihood of a snow storm is a risk. Another related term is vulnerability. We are vulnerable because we are not well positioned; for example, we are more vulnerable to getting sick if we don’t have enough sleep. Vulnerability, therefore, means the extent of risk resulting from a weakness.

BUSINESS CRITICAL SYSTEMS

Organizations should understand the risks related to every business critical system. A business critical system is one that is needed for the organization to conduct business without significant interruption. These systems can range from common tools like email or a web site to more specific systems like supply chain or automated teller machine (ATM). Often one might question what systems are not business critical. Those systems

should be few. The more systems are not business critical, the less efficient the organization is. Some are inevitable, and although not business critical, are beneficial to the organization, e.g., an employee suggestion system.

Business critical systems should be determined based on the nature of the organization's business mission. For example, banking systems are critical to a bank, a supply chain management system is crucial to a company like Walmart and a water quality system is essential to a city government. In addition to the function of a system, the transaction volume and total value of assets managed by the system should be major criteria in determining business criticality.

INHERENT RISK

The more vulnerable an asset is to errors, loss or damage, the greater is the inherent risk. Similarly, the greater the magnitude of vulnerable assets or transactions processed by a system, the higher is the inherent risk. An extension of this is that the more widespread a system is, e.g., an Internet facing system, the greater is the inherent risk. A wire transfer system that handles a large volume of high dollar transactions daily is riskier than a payroll system because it involves many user organizations in an online environment and improper transactions can be difficult or too late to reverse. Other factors affecting inherent risk include the legal implications of errors, the potential repercussion in terms of customer goodwill and adverse effect on competitiveness.

Inherent risk has three components: the probability of an unfavorable event, the nature of damage and the extent of damage.

The following factors should be considered in performing inherent risk assessment:

- Age of procedures.
- Age of the system.
- Business criticality of information technology.
- Method of information storage (on site, off site, network, outsourcing etc.)
- Nature of information processed (e.g., value and frequency of change).
- Nature of people (experienced or inexperienced, consultants vs employees).
- Nature of processes (e.g., batch or online).
- Nature of systems (e.g., complexity, Web enabled, and geographical diversity).
- Past experience.
- Stability of system.
- Staff turnover.
- Transaction volume.

Management is responsible for assessing and mitigating inherent risk. The following steps can be followed in risk assessment.

1. Identify the significant and potentially unfavorable events for which a solution requires management decision from event to event. Significance, of course depends on quantitative exposure and probability. Quite often, however, significance can be assessed intuitively based on experience and it is quite easy to

rule out far fetched and really trivial exposures. An example of the former is a risk for which the organization has no control, e.g., World War III. An example of something trivial is an occurrence that can be easily addressed without significant service interruption or loss of assets, e.g., employee tardiness. Some significantly unfavorable events may not be far fetched or trivial but the solution is quite standard across the industry, e.g., the risk of virus infection. In this case, it is a "no brainer" for organizations to deploy commercial anti-virus software on each computer and update the virus detection files as they become available from the anti-virus software vendors. If an event type is within an organization's control, is not trivial and, is not already addressed with an accepted and standard risk mitigating practice, the organization should put it on the list for risk assessment.

2. Assess the damage of each event (not each occurrence). An example of an event is server breakdown. The breakdown of a server or a group of servers simultaneously is an occurrence. Some events and occurrences are interdependent. For example, when a server breaks down, it increases the probability that another server in the cluster will break if the load is shifted to other servers in the cluster. On the other hand, a broken server cannot be hacked. These chain effects have to be considered in risk assessment. Estimate the average magnitude of each event based on organization and industry experience. For example, how long will it take to fix or replace a server?
3. For damage leading to financial loss, estimate the amount of loss from each occurrence of each event. Take into account the chain effect between events. Damage should be quantified as much as practical. The relevant transaction volume, relevant asset value maintained, contractual obligation as well as organization and industry experience in legal liability should be used to estimate the financial loss. If an estimate is soft, it can be discounted to arrive at a quantified estimate, e.g., if an occurrence of an unfavorable event will likely lead to the loss of a major customer, a subjective likelihood of say, 20%, 30% can be applied to the annual profit from the customer.
4. Estimate the probability of each event (not each occurrence). For example, if the risk of a computer breaking down on a given day is .005%, the annual risk is 365 x .005%, i.e., 1.825%. Well, what period should be used to quantify the risk? It should not be too long like several years, nor should it be too short like daily. The common time cycle used by organizations to plan and report financial performance is annually. Therefore, it seems practical to express the probability of unfavorable occurrence on an annual basis.
5. Based on probability, estimate the number of occurrences per year. This would also depend on the nature of the event. The denominator unit for the probability should be chosen based on practicality and strong relevance to the event whose risk is being assessed, and it should be clearly stated. Here are some examples:

a. If the probability of hacking is 0.01% per server per day, the estimated number of hacking incidents would be 3.65% per year per server. This sounds high but the logic is right. A common analogy is our chance of catching a cold. I catch a cold once a year, so on average, my risk of catching a cold is 1/365, or 0.274%.

b. If the probability of a ghost employee (a recorded employee receiving pay who does not exist) is 1% of the total number of employees, the number of ghost employees on an annual basis would still be 1% of the average number of employees. This is because the first probability is not expressed in relation to a time frame.

c. If the probability of processing a claim payment in the wrong amount is .01%, the number of incorrect payments in a year would be .01% of the total number of payments in the year. Here, the probability is unchanged because both values are expressed over the same period. However, the number of incorrect claims will change because the annual number of claims is a high number compared to only one claim being processed at a point in time.

6. Multiply the estimated number of occurrences by the estimated financial loss from each occurrence to arrive at the financial exposure from the unfavorable event. The above examples are extended as follows:
   a. If the estimated financial loss of an average hacking incident is $10,000, the financial exposure on an annual basis is $365 per server. This amount should then be multiplied by the number of servers. Some servers are more critical, so the organization can apply a varying degree of granularity in this calculation.
   b. The estimated financial exposure from ghost employees can be calculated as 1% of the average number of employees multiplied by the average salary, or more directly, calculated as 1% of the year's payroll.
   c. The annual financial exposure from incorrect claims payment can be estimated as .005% of the total amount of claims paid in a year. The probability of .01% in step 5 can be converted to .005 % because a mistake can go either way. An overpayment may not be recoverable, whereas an underpayment would most likely be brought to the attention of the organization by the payee. In addition, the cost of reprocessing has to be estimated. These factors have to be considered.

7. Add all the financial exposures for the identified potentially unfavorable events for each business critical system.

8. Rank the business critical systems by financial exposure.
9. Use the financial exposure as a gauge to decide how much internal control to design and implement, taking into account the cost of designing, implementing and operating each internal control. An internal control should be designed and implemented only if the financial impact of the risk to be mitigated outweighs the cost of the control. This means internal controls should be implemented to provide reasonable assurance of system reliability, as opposed to absolute assurance.
10. The financial exposures of all business critical systems can be added to assess the organization's exposure to unreliable systems.

Some would say that the above steps are onerous and subject to judgement. Risk management is judgmental, but based on informed judgement in observance of corporate guidelines. The steps can be automated. As many of the parameters can be standardized and automated as practical, based on experience and industry statistics. The remaining parameters like error rates should be estimated by managers with consultation and following corporate guidelines that provide criteria and examples.

Identifying Potentially Unfavorable Events

Management should use the CAATOE attributes that we talked about in the last chapter to identify potentially unfavourable events.

- Completeness
- Authorization
- Accuracy
- Timeliness
- Occurrence

The following simple matrix can help to assess inherent risk.

Risk Matrix

	Completeness	Authorization	Accuracy	Timeliness	Occurrence
Input					
Processing					
Output					
Storage					

This matrix shows that an unfavorable event can occur at the input, processing, output or information storage phase of a transaction cycle. Such an event may include information change or access that does not reflect a real transaction, incomplete, inaccurate or untimely transaction processing, the processing of an improperly authorized transaction, or processing transactions inefficiently in relation to the cost of processing including the cost of hardware, people and software.

Each cell should be addressed in relation to the system being risk assessed. In addressing each cell, management should consider the five system components, i.e., infrastructure, software, people, procedures and information. Management has to think about what can go wrong with each component during each stage of the transaction cycle (input, processing, output and information storage) with respect to each risk attribute (completeness, authorization, accuracy, timeliness and occurrence). To document such risk identification, a number of matrices can be prepared, e.g., one matrix for each system component or one matrix for each subsystem of a system.

Completeness

Incomplete processing will result in incorrect accounting records, loss of revenue, unhappy customers or unhappy users. This can happen because of incomplete input, faulty programs that miss some transactions, invalid data that causes transactions to be rejected and lost, hardware failure, interception of computer processing by hackers, or rogue systems administrators. Here are some examples of incomplete processing.

- An automated banking machine (ATM) fails to capture the last digit of an amount entered although the correct amount is shown on the screen. This can easily occur because of hardware malfunction. Preventive maintenance is a control to mitigate this risk.
- A database fails to record a large amount because of field overflow. This can be a type of buffer overflow which is a common system design flaw. Rigorous system testing can help mitigate this risk. This is described more in Chapter Eight.
- Incomplete input procedures resulting in some transaction data not being entered. Detailed user procedures would help mitigate this risk.
- eBusiness customers do not enter all necessary data. The risk is high because people these days are always in a rush. System edit checks should prevent this.
- Incomplete database update because of program flaws. This risk increases as organizations continue to implement enterprise resource planning systems that update multiple database tables based on single data entries. One control that can help mitigate this risk is a database referential integrity check. This means checking that a foreign key is not blank for any record.

Accuracy

Little writing is needed for one to appreciate what inaccurate information can lead to. We live in an information intensive society. Many people have a habit of turning on the TV to check the day's weather forecast, especially in the winter, to decide what to wear and which route to take to work or school. A store manager will log on to the computer to check the promotions for the day and the sales figures for the previous day, this information will affect how s/he operates the store. A foreign exchange trader will check the rates and trading positions many times a day. When information is wrong, the effect may be minor on a personal basis, or it can be devastating to an organization. Computers have been known to be wrong because of hardware failure, program flaws or human

errors in operating the computers or feeding data. Errors may appear in input data, such as in customer names or numbers. Alternatively, they may appear during processing, for example, when a system incorrectly multiplies quantities ordered with unit prices. Some common mistakes are:

- Transposing two digits when entering a social insurance (security) number is a common occurrence. A mitigating control is to use a check digit algorithm, i.e., a system computing the derivative of say, the first 8 digits of a social insurance (security) number to form the last digit and then compares the computed last digit with the input last digit. This control will work if the social insurance (security) system uses this formula when assigning the numbers in the first place.
- A software error leading to wrong calculation, e.g., the Excel bug that was discovered in 2007. Rigorous system testing would be the preventive medicine.
- Entering a wrong amount. For example, accidentally hitting the minus sign. A system edit check can detect this.
- The system looking up the wrong payroll deduction code from the deduction table. System testing would be an effective preventive control.
- Affixing incorrect bar codes on products. Many of us has experienced that when we find out we have been overcharged or when we have to wait at a cashier counter until the correct price is accepted by the system. Verification of bar codes before being rolled out to operation is a preventive control for this type of errors. Using a check digit formula as explained above to validate stock ID numbers before bar code conversion is another control, e.g., if 12345 is a valid ID number because it satisfies the formula of the sum of the first 4 digits divided by 2, then 12346 is an invalid number and should not be converted to bar code.

Authorization

Unauthorized transactions can cost an organization immensely. For example, Société Générale', a large bank in France, took a significant market loss when it liquidated unauthorized trades in 2008. Unauthorized access to sensitive information can also be damaging to an organization. Imagine a disgruntled employee posting customer credit card numbers on the Internet.

Transactions may be carried out without authorization, or with inadequate authorization. Changes to master files may be made without authorization. There are two elements to this. First, there is no authorization from the person accountable for the transaction or data file. For example, a payroll clerk changes someone's salary without management approval. In this case, the payroll clerk has the system authority to make salary changes, but s/he does so without following documented procedures. Another way transactions are entered without authorization is when someone circumvents system security by say, breaking a password or impersonating an authorized user. Some other examples of unauthorized transactions are:

- Write-off of accounts receivable from a friend.
- A payroll clerk overstates his or her own hours worked.
- An accountant puts through a journal entry that exceeds his or her financial limit.
- A customer accesses another customer's account.
- A programmer changes programs without approval.
- A customer service representative or auditor reads customer information for personal curiosity beyond their duty or audit requirements.

Common internal controls to mitigate the above risks are restricted access and access audit trail review.

Timeliness

To most organizations, information is money. When information is not current, incorrect or ineffective decisions are made. Organizations might even incur liability. The reason for late information may be untimely processing, tardy reporting or a system failure.

Sometimes data may be incompletely input or processed only temporarily. This means although data eventually gets into the system, it is late, and in some cases, too late, resulting in unreliable information or loss to the organization. Here are some examples of untimely transactions:

- Recording sales weeks after shipments leading to cut-off errors. Regular reconciliation can help to detect this.
- Removing employees from payroll long after departure resulting in overpayment. A rigorous exit checklist should be used.
- Late in sending out T4s or W2s, leading to penalty from Canada Revenue Agency or Internal Revenue Service. Regular monitoring of computer processing schedule should be performed.
- Late in recording inventory receipts resulting in an incorrect inventory balance. Regular matching of invoices to receiving reports would help to detect this.
- Late in paying invoices resulting in loss of cash discounts or a supplier. Accounts payable should be aged and reviewed by management.

Occurrence

Information may be processed that does not represent real transactions. This can also mean information being processed by a faked system. Here are some examples of what can go wrong.

- A faked ATM luring customers to insert their ATM cards. The risk is likely to be low because of the significant investment to set up a faked ATM. Regular bank inspection and customer education would help to mitigate this risk.
- A fictitious web site can lure customers to provide identity information and the criminal can then transact using the stolen identity. A control to mitigate this risk is to use digital certificates, which is a kind of electronic business card downloaded by a browser to verify a web site's identity. We will discuss this more in Chapter Eight.
- An employee downloads a malicious program that appears to be useful software. This is quite common. Anti-virus software can be an effective control.
- A payroll clerk sets up a ghost employee. This is one of the older tricks to commit fraud and is still used frequently. It requires little technical knowledge and can be achieved with just ordinary payroll system privilege if the person doing this is a payroll administrator. A standard control to mitigate this risk is the requirement for management review.
- Entering payroll hours that were not worked. Many organizations would admit that this occurs. Management review can be an effective control.

The Effect of Information Technology on Inherent Risk

Certainly, automation reduces human errors. Replacement of manual functions can make it more difficult to collude to commit fraud, especially for people who are not IT savvy. A computer does not get sick and tired so it is more likely to finish its jobs on time. Computers do not go on strike, although computer staff could. These factors reduce inherent risks. However, one might be under pretence to think that increasing automation will reduce the extent of improper transactions. This theory, as proved by experience, is not true. The reason is that computers are controlled by people. The fewer people are involved, the less cross-checking or observation there is to deter people from carrying out improper activities. Therefore, increasing automation generally increases the risk of fraud.

Electronic transaction trails are less visible and create more uncertainty. Access is more difficult to control. There are more parties having access to corporate information. There is less time to react to errors. There is a higher risk of information loss because of the concentration of storage. Because of the concentration of processing function and connections, power outage or network failures can cause the systems to be unavailable on a massive scale. Such impact would materialize to a lower degree for manual processes. These factors serve to increase inherent risks. Here are the common risk factors in information systems.

Concentrated Processing

In computer systems, the processing is often concentrated within computer facilities. Certain organizational units are bypassed during processing operations. Consequently, less opportunity exists for detecting errors and fraudulent events such as unauthorized transactions, changes in programmed instructions and theft of assets. Current IT practices such as virtualization will concentrate computer processing even further.

Less Reliable Audit Trail

The audit trail is more likely to be fragmented or eliminated. Source documents may not be used, for instance, when sales orders are taken over the phone, they are entered to the system directly. Sometimes there might not even be verbal communication, the transaction initiator puts in to the system what is in the mind; if there is a need to seek justification, where is the audit trail?

Human Judgement Bypassed

Computers perform programmed instructions blindly, i.e., they exercise no judgement. Therefore, fewer opportunities exist for people to spot errors and question data. For example, a pricing error on the web site of a major retailer resulted in the sale of 600 units of a product in a day which were significantly underpriced because of a web price catalog input error.

Data Storage not Visible to Human Eyes

Data stored in computer systems is oriented to the characteristics of digital media. These characteristics differ from the paper oriented and hence human oriented media. Data, when stored in these devices, is not comprehensible to the human eyes. It is necessary for users to take steps to retrieve the data and decipher it using software so it can be interpreted. While this may add to security, the extra steps introduce room for errors.

Data is easily erasable without leaving a trail. A disk can hold millions of records and damage to the disk because of humidity or demagnetization can cause all of these records to be lost. Similarly, if the disk is lost or if an authorized person gets hold of it, a lot of information can be compromised or destroyed.

Other Common Causes of Inherent Risk

Here are some other common causes of IT risks.

1. Management does not understand IT. It is easier for management to understand business issues and even financial issues. Because of their lack of understanding of information systems, executives often rely on the IT department to tell them how much money is needed. This can make IT investments subject to less scrutiny than other expenditure, and can lead to ineffective spending.

2. Employees do not understand IT. Information technology often facilitates business process reengineering that changes jobs in organizations. Mundane and clerical jobs may be eliminated or replaced with jobs that require higher skills in order to support an organization's goal to expand. Employees who are moved to new jobs may not understand the technology required to do their jobs. Many organizations do not do a good job in training their employees for change. This makes the use of IT more erroneous and ineffective.

3. Increasing use of IT means more processes are integrated. In such a case, the weakest link in the chain can drag down a number of functions. Complicated systems are also more difficult to understand and maintain.

4. More and more organizations are sharing systems with real time information transfers between business partners and vendors. For example, some retail giants open their inventory systems to suppliers to query and automatically send replenishments, avoiding the paper work of purchase orders. The risk of divulging trade secret is higher and organizations may have to rely on systems in which they have no control.

5. Electronic information is easier to steal and there may not be a trail. It is difficult for organizations to know whether an employee has copied sensitive files to memory sticks to be given to competitors.

6. IT changes rapidly and even technical people find it hard to keep up. Computing power doubles every year. Managers are always called by vendors to try new products. Some vendors also use fear tactics to convince management that the options are to upgrade or lose support or competitiveness. Organizations may therefore be talked into making incorrect or excessive purchases. On the other hand, organizations that fail to upgrade may indeed be less competitive. Knowing where to spend IT money is challenging and something managers must pay close attention to.

7. More and more organizations outsource IT functions so they can focus on their core businesses. Governments and large companies have outsourced in order to be more cost effective. Common functions that have been outsourced include payroll, accounting, network support and call centers. When an organization outsources, it loses some control. If the service provider makes mistakes, it will impact on the user organizations and they sometimes are caught by surprise. Even without outsourcing,

every organization uses an Internet service provider. We hear of ATM failures from time to time; some of them may be the result of system failure of the network service providers.

8. Computers can make managers less productive. Managers who are less technology savvy may spend an inordinate amount of time learning to use systems and this may make them neglect their main function, to manage. On the other hand, more technology oriented managers may really enjoy using technology so much that they treat computers as toys, so as a result, they may spend too much time exploring system functions or surfing the net beyond what is needed to perform their jobs. They may even get a lot of satisfaction in developing their own systems to solve business problems and thus become highly paid programmers who write inefficient or ill-controlled programs.

9. Knowledge management is another common risk factor. To keep up with technology changes, organizations have to invest in training their staff members. A lot of organizations are willing to buy new tools but do not give their staff enough time to attend courses to learn to use the tools; as a result, IT investment is not returning the desired benefits.

10. Many organizations place heavy reliance on long-term IT employees who over the years have accumulated detailed knowledge of the systems used in the organization. When these employees leave, the organization may experience system problems unless there is proper knowledge transfer. For example, many large organizations still rely significantly on systems written in Common Business Oriented Language (COBOL) and Programming Language 1 (PL1), two common mainframe programming languages. Many universities have stopped teaching these languages. Many mainframe programmers have retired or are close to the retirement, so when they leave, there will be a knowledge gap. To some extent, organizations can address this problem by acquiring middleware to bridge web interfaces with legacy systems and make the legacy code (programs) more graphically oriented for younger programmers to maintain. There is still a need to ensure a critical mass of legacy programming skills until organizations replace their mainframe systems. At the other extreme, some organizations are routinely selecting younger workers in hiring and promotion over experienced candidates just to develop a youthful work force. Both of these extreme approaches increase the organization’s risk to inaccurate and unauthorized transactions.

11. Because of the high turnover of IT staff, organizations sometimes find it necessary and more flexible to hire consultants, especially when an organization is under a hire freeze for full-time positions. Consultants may not have much knowledge about the organization and its policies. They are more expensive than employees. They may not be as dedicated as employees so in a crisis, the organization may be caught without the necessary staff to solve problems.

12. The needle-in-a-haystack problem will occur more frequently when IT is used. For example, a small program bug can cause erratic information errors. Some program bugs may only be triggered by certain factors and they may take years to be discovered, but when they are active, the impact could be very significant.

Risks of Database Systems

A database improves efficiency and avoids data redundancy. However, data sharing between applications increases the risk of unauthorized access and update errors. The more programs that can update a table, the more likely errors will occur. Also, because more system software is used in a database environment, the risk of incorrect software configuration increases. Database applications often are operated in a distributed network. In that case, there are multiple copies of a database geographically dispersed. It is important to ensure that updates are synchronized. It is just as important to ensure time synchronization, by for example, operating a time server. Because a database consists of many tables that are shared between applications, there is also a risk of data inconsistency between tables when data is repeated unnecessarily, e.g., a customer address shows up in multiple tables but is represented inconsistently. This risk results from data redundancy. There is also the risk of concurrent updates, i.e., one transaction overwriting the result of a previous transaction. We will discuss internal controls to mitigate these risks in Chapter Six.

Concurrent Updates

In a database environment, programs sometimes contend for the same table and field in terms of reading and writing. Although technically, the hardware will not allow two programs to update a field at the same time, just as it would be impossible for Magic Johnson and Yao Ming to enter a 3-foot wide doorway in parallel, there is a risk of updates performed by two programs almost concurrently that could impair data integrity. Here is an example.

I deposit a $1,000 check at an ATM to a joint checking account. Less than a second later, my wife transfers $2,000 from the checking account to a saving account using eBanking. Before these transactions, the checking account balance is $5,000. Here is what could happen.

1. My transaction reads the $5,000 balance and updates it to $6,000.
2. My wife's transaction reads the $5,000 balance (after my transaction has read it but before my transaction finishes) and calculates a new balance of $3,000.
3. My wife's transaction finishes after mine, so it overwrites the new balance as $3,000.
4. In fact, the correct balance should be $4,000.

This is called concurrent update. That is, two transactions update the same field of the same record without knowing about each other. In other words, the left hand doesn't know what the right hand is doing. To prevent this kind of data inconsistency, organizations should configure database management systems to enforce record locking. We will describe this in further detail in Chapter Six.

CONTROLLING INHERENT RISK

Management can control inherent risk in three ways. Management can avoid inherent risk by refraining from the practice that will generate the risk, e.g., by not offering eBusiness. If risk avoidance is not desirable, management can transfer the risk by buying insurance or engaging a partner to assume all or some of the risk, e.g., an insurance company can sell some insurance policies to a reinsurance company to offload some risk. The third approach is to implement internal controls to mitigate the risks. *An internal control is an established procedure, instruction or tool to mitigate inherent risk.* The procedures may be automated or manual. These three ways are not mutually exclusive.

Inherent risk depends on the nature of business, the nature of assets, as well as the environments in which business is conducted and assets are stored. Management can avoid inherent risk by not going into a certain line of business, staying away from certain products and being more cautious and conservative in choosing locations. Doing so, of course, may limit the organization's growth and profitability and increase cost. There is often a direct relationship between risk and reward. Management wants to strike an optimal balance by doing risk assessment. This is why although large organizations should charge their executives with the responsibility for controlling business risks, these organizations often have separate risk management departments and chief risk officers to coordinate effort in risk management.

To mitigate inherent (business) risk, management should implement internal controls. The remaining risk net of risk reduction by internal controls is called residual risk. Residual risk should be at a level management considers acceptable. The implementation of internal controls should stop at a point where the marginal cost of internal controls will exceed the financial exposure to be reduced. Organizations should have guidelines to help managers measure the cost and benefit of internal controls. The benefit of internal controls is the extent of inherent risk to be reduced by the controls.

Before deciding whether a risk should be avoided, shared or mitigated, management should assess the significance of the risk. What is significant to one manager may not be to someone else. Therefore, an organization should have a formal risk assessment and acceptance policy in terms of significance. The thresholds should be quantified as much as practical. The degree of granularity of risk quantification and significance assessment should also be indicated in guidelines within the risk assessment and acceptance policy. In other words, should the risk of equipment failure be expressed as per incident, per piece of equipment, per year etc.?

The risk assessment and acceptance policy should specify the monetary levels of risk that can be accepted by each level of manager. Most organizations have documented levels of signing authority for expenditure. For example, a first line manager can make an individual purchase of up to $50,000. However, many organizations do not have a similar policy for risk acceptance. Auditors often get a statement from managers that they are accepting the risks. But can a middle manager accept the risk of asset loss amounting to $1 million, even if this amount is within the annual budget of the manager? Financial service companies have rigorous signing levels for approving loans. More organizations should move towards implementing a policy for risk acceptance for operation risks including IT risks.

Internal auditors should assess inherent risk using the corporate policy. If such a policy does not exist, internal auditors should recommend that it be established. Meanwhile, internal auditors should assess inherent risk in relation to the business strategy for the organization and then for different departments. What is important to management is important to internal auditors.

Shareholders' auditors should assess inherent risk in relation to materiality in the context of the financial statements. Shareholders auditors are concerned about the completeness, accuracy, authorization, timeliness and occurrence of recorded financial information. They are not really concerned about efficiency or lost profit as long as the financial records have integrity. Where a risk is determined to be significant, shareholders' auditors will look for internal controls for mitigation.

In this book, we focus our risk discussion on IT, i.e., the risk of operating inadequate or unreliable information systems. This is a subset of managing overall business risk, which includes vision, strategies, monitoring, innovation and cost control. These activities depend on the reliability of information produced by systems. Even if transaction processing and management information systems are highly reliable, a company may not be managing business risk competitively if its products are not efficient or fall behind competitors' in terms of innovation and market acceptability, e.g., competition in the smart phone market. Management should realize that competitive product development and sales activities depend on the reliable and efficient information systems.

CONTROL RISK

Management has to design and implement internal controls to mitigate risk. For an asset or system to be managed, there is a risk that the internal controls will fail to reduce inherent risk to the extent desired. This risk is called control risk. The following control factors contribute to control risk:

- Inadequate assessment of inherent risk resulting in designing the wrong controls or weak controls.
- Designing internal controls that are too hard to follow.
- Designing internal controls that are too vague and subject to inconsistent interpretation.
- Designing internal controls that are carried out too infrequently or that use small samples
- Inadequate or improper implementation of internal controls, e.g., incorrect programming.
- Inadequate compliance with internal controls because of insufficient procedures, training and monitoring.

Most of the factors that affect inherent risk also affect control risks. Here are some examples:

- The speed and inherent accuracy of a computer makes automated controls more reliable than manual controls.
- Increasing automation involves fewer people in transaction processing and therefore makes it harder to segregate duties for cross checking. This increases control risk.
- Electronic trail of transactions also makes the trail of control activities less visible and more prone to being erased. This increases control risk.
- Higher concentration of transaction processing also results in higher concentration of internal controls in fewer servers. This "putting more eggs in a basket" increases the risk of internal controls failure.
- Increasing automation often involves more reliance on trading partners and service providers to carry out internal controls. This increases the risk of controls not being carried out properly because the organization has less control over controls.
- Outsourcing puts some internal controls in the hands of a service organization and because the user organization has no or less influence over the controls, the risk of internal controls being inadequate or ineffective increases.

Management should minimize control risk by involving business units and internal auditors in risk assessment, designing rigorous and redundant internal controls, and monitoring internal control compliance. The level of control risk tolerable to management and internal auditors is low.

Shareholders' auditors generally tolerate a higher level of control risk, it is generally moderate. Moderate does not mean 50%. Accounting firms have a range that they apply to different industries and it can probably range upward to say, 40%. Shareholders' auditors accept a moderate level of control risk because their audit opinion is not on internal controls, but rather, on the fairness of presentation in the financial statements.

There is an exception, Canadian and U. S. public companies have to report on internal controls supporting the financial statements to securities regulators and shareholders' auditors are usually asked to provide an opinion on the controls. In this case, the shareholders' auditors will tolerate only a low level of control risk.

RESIDUAL RISK

Residual risk is the product of inherent risk and control risk. Assume that in an organization, the inherent risk of setting up a ghost employee in the payroll system is 1%, i.e., without any internal controls, management estimates that the probability of a ghost employee being set up is 1% based on industry and organization experience. Management has now implemented internal controls to mitigate this inherent risk. Assume that management has estimated the risk of the internal controls not being adequate and effective is 5%. The residual risk is now .05%. If this is not acceptable, management will have to improve internal controls to lower the control risk. The inherent risk cannot be changed unless management decides to make structural changes to the payroll system like centralization.

Management should assess and accept residual risk in the same manner as its assessment and acceptance of inherent risk. This is because residual risk is simply a reduced degree of inherent risk. The organization policy on risk assessment acceptance with different sign-off levels should apply to residual risk. That is, when a residual risk exceeds the level of authority of a manager, s/he should implement further internal controls to lower the risk. If the cost of the controls exceeds the amount of the risk to be mitigated, the manager can in theory accept the risk. However, if such a risk exceeds the manager's approval authority, s/he should refer it to a higher level of management to understand, assess and accept the risk.

Internal auditors should assess whether management's tolerable control risk is appropriate given their assessment of inherent risk. If it is not, the internal auditors should raise their objection to management with explanation and raise it with the audit committee if management's tolerable control risk is significantly higher than what the internal auditors think it should be. If management's tolerable control risk is appropriate, the internal auditors will have to confirm that the control risk is actually at that level. Such confirmation will require studying internal controls to assess their reliability on paper and then testing internal controls. The extent of testing will depend on the control risk. The higher the tolerable control risk, the lower the acceptable control reliability, and the smaller the samples will be used in testing.

External auditors of financial statements will take a slightly different approach in assessing control risk. We will discuss that under Audit Risk.

RISK REGISTER

An organization should maintain a consolidated list of inherent risks and residual risks segmented by lines of business. This register should indicate the risk owners, risk weights, risk ratings and exposures. The list of inherent risk is used to regularly assess the adequacy and redundancy of internal controls. The list of residual risk points to the actual exposures faced by the organization and it is also used to assess the effectiveness of internal controls in operations. The owner of the risk register is the chief risk officer, whereas individual risks are owned by the line executives or the CIO depending on whether a risk is related to a business area or the IT infrastructure.

The chief risk officer should develop and maintain the risk assessment and risk acceptance policy as well as supporting procedures to ensure consistent risk assessment in the organization. This executive should also provide a center of excellence in risk assessment. To maintain the risk register, the chief risk officer has to coordinate periodic risk assessment and ensure that the findings are addressed with internal control improvements. There should be a corporate risk report broken down by business line and types of risks (e.g., IT, credit, market) submitted to senior management at least annually. In a major North American bank, the chief risk officer is a vice-chair responsible for the coordination of assessments of credit risks, IT risks and operation risk. She is also responsible for insurance (to protect bank operation and liability) and internal audit.

MANAGEMENT CHECKLIST

1. Senior management should appoint an executive to coordinate risk assessment throughout the organization.

2. Senior management should develop a risk assessment framework consisting of risk factors, weighting criteria, weight scale, risk assessment scale (e.g., 1 to 10), frequency of risk assessment and a prioritized list of critical systems.

3. Senior management should charge each executive with determining his or her business critical systems.

4. Compile and prioritize the business critical systems for the entire organization.

5. Provide regular risk assessment training to managers.

6. Provide an annual or quarterly risk profile report to the board of directors.

7. Maintain a risk register in the organization which details the financial exposure of each business critical system and each business area. A business area may use more than one system and a system may support more than one business area. Financial exposure in the risk register in turn is supported by quantitative assessment of inherent risk and control risk.

8. Perform annual benchmarking with the industry on the organization's risk profile.

9. Ensure that the risk profile of the organization is appropriately disclosed in the annual report to shareholders and relevant stakeholders.

10. Include a risk assessment section in the business proposal for every IT project.

CONCLUSION

Because of the uncertainty in audit trail completeness as well as the increased difficulty in understanding and controlling electronic processes and access compared to less automated processes, the overall risk impact of information technology is that it generally increases inherent risk, control risk and detection risk. Organizations are increasingly realizing the importance of structured risk management as evidenced by the growing number of large organizations that have appointed chief risk officers. There is also a positive and encouraging trend to include IT risk assessment in the job description of the chief risk officer.

REVIEW QUESTIONS

1. How does automation affect segregation of duties?

2. What do you see are the responsibilities of a chief risk officer?

3. What are the risks of an ATM (banking) system?

4. Describe the risk of cloud computing.

CASE – Everbright Industries

Everbright Industries manufactures and sells solar panels. There are no retail sales. Customers include retail stores and building contractors. The company employs over 1,000 workers in two shifts, and most employees work overtime when necessary. Everbright has had major growth in its production and has recently acquired and implemented the Axiom enterprise resource planning system to handle payroll, standard product production costing, job order cost accounting, order processing, inventory management, production planning, distribution operations, and financial accounting. Gerard Chung, president of Everbright, has recently asked the shareholders' auditors to give him a report about the Company's business and operations risks. As the accounting firm manager taking on this assignment, you have learned the following in the first week. Other executives include:

- CFO: Jill D'Anna
- Chief marketing officer – Chuck Slick
- Chief engineer – Rohan Nerd
- Vice-president of manufacturing – Gary Sturdy
- Director of warehouses – Bob Fail.

The two warehouses are in Markham and Mississauga, Ontario, Canada. The Company Head Office is in Markham, where the warehouse is. There are two branches in Montreal and Vancouver. In 2013, sales totalled $75 million; unaudited gross profit is $32.3 million and unaudited income before income taxes is $12 million.

1. Orders are taken by the sales representatives who are always on the road. Two of the sales reps are in Montreal and bilingual. In addition, the president and the vice-president of marketing often take orders directly and assign them to the director of warehouses to fill.

2. The Axiom system is intranet enabled. The sales reps, the president, Jill and Chuck have read and update access via transaction menus. Orders over $100,000 are reported the next day to Gerard.

3. The Company does not use standard costing. Orders under $100,000 are cost based on the first-in-first-out method. Large orders use cost assigned by Jill.

4. The Axiom system is operated out of Head Office. The server in each Branch office is connected to Head Office via secure Internet (virtual private network with encryption). The 3 desktop computers in the Mississauga warehouse are also connected to Head Office via VPN. There are no IT staff outside of Head Office. The IT department consists of the manager, 2 analysts, 2 programmers (whose jobs consist of supporting the Axiom system and Web hosting), 2 system administrators. The IT manager reports to Jill.

5. There is a web server but no eBusiness. There are 2 parallel Axiom servers, 2 parallel database servers and 1 network server for email and shared drives.

6. All manufacturing is done in Markham.

7. In some cases, rush orders and special orders have been filled partly using finished goods from a company owned by Gerard's brother-in-law, in China. This accounted for 5% of sales last year.

8. Gerard wants to launch eBusiness and he will use your risk report to help him formulate the plan.

9. The human resources (HR) department determines the wage rate of all employees. An HR specialist starts the process by sending an authorization form for adding an employee to Jennifer Desousa, the payroll coordinator. After Jennifer inputs this information into the system, the computer automatically determines the overtime and shift differential rates for the individual, and it updates the payroll master files.

10. Employees use access cards to record the hours worked. Every Monday morning, Jennifer uploads the daily start and finish times for the previous week to Axiom.

Required

Describe the general and IT related inherent risks. For the IT risks, suggest mitigating practices.

RUNNING CASE - Blackberry

1. Develop a risk register for Blackberry to include 5 key strategic and 20 key operation risks. Describe the risk mitigation practices.

2. What are the key business risks faced by Blackberry and how to you think the Company is performing in addressing these risks?

3. If you were the CEO, what would you do to rescue or salvage Blackberry?

MULTIPLE CHOICE QUESTIONS

1. Which of the following is most likely to cause privacy breach?
   A. Enterprise resource planning system
   B. Batch systems
   C. Customer relationship management system
   D. Managing and retaining data

2. Which risk is best mitigated by a database management system?
   A. Occurrence
   B. Privacy
   C. Integrity
   D. Authorization

3. Which is the right formula for residual risk?
   A. Inherent risk x detection risk
   B. Inherent risk x control risk
   C. Control risk x detection risk
   D. Control risk – audit risk

4. Which risk increases the most with virtualization?
   A. Program errors
   B. Data entry errors
   C. Improper data access
   D. Data redundancy

5. What will happen if two bits are altered during data communication, i.e., a 0 becoming a 1 and vice versa?
   A. The transaction will be incorrectly recorded.
   B. Confidentiality will be breached.
   C. The network will be jammed.
   D. The message will be intact because of the offsetting errors.

6. “Passwords may be easily broken.” This is a(n):
   A. inherent risk.
   B. weakness.
   C. control risk.
   D. conclusion.

7. “With the current infrastructure, we stand to lose $2 million of business a year as a result of system breakdown.” This is a(n):
   A. exposure.
   B. conclusion.
   C. residual risk.
   D. accepted risk.

8. A manager creates an Excel spreadsheet for his staff members to enter hours worked. The spreadsheet is then imported to the payroll system. What is the greatest risk?
   A. Staff getting paid for hours not worked.
   B. Employees may see the numbers of hours worked by others.
   C. Staff do not enter hours worked.
   D. The spreadsheet is not signed by employees.

CHAPTER THREE – IT GOVERNANCE AND GENERAL CONTROLS

"He who controls the present controls the past. He who controls the past controls the future." - George Orwell, author and journalist.

We have talked about information technology (IT) risks in the last chapter. To mitigate risks, organizations should put in place a system of internal controls. The system of internal controls actually is not a stand-alone system, rather, it contains internal controls that work their way into normal transaction processing, in order to be effective on an ongoing basis.

The extent of internal controls to be designed and implemented depends on risk assessments. Based on the result of assessments, internal controls should be implemented to address the five components of a system: infrastructure, software, procedures, people and information. Controls should be implemented to mitigate the risks of lack of authorization, inaccuracy, incompleteness, untimeliness, fictitious information and inefficient processing. Controls have to span the entire transaction cycle of input, processing, output and information storage. We repeat here the risk matrix which should be used to ensure controls address the transaction cycle and risks.

	Completeness	Authorization	Accuracy	Timeliness	Occurrence
Input					
Processing					
Output					
Storage					

Internal controls to address the above can be manual or automated. Most manual controls also involve system generated information. The Y axis of this control matrix is more useful for developing internal controls that directly address a transaction cycle, i.e., application controls. Application controls are internal controls that apply to a specific business system, e.g., an edit check of a student number. The transaction cycle is less relevant to developing infrastructure controls, also called general controls. A general control applies to multiple systems, e.g., a network password. The matrix, on the whole, is useful for both general and application control development. We will discuss general controls in this chapter and application controls in Chapter Six. Internal controls are designed and implemented to provide reasonable assurance that risks are contained. This means the cost of control design and execution must not be higher than the financial and imputed cost of intangible risk should the risk materialize.

DEFINITIONS OF INTERNAL CONTROL

An internal control is an established instruction, tool or procedure to mitigate risk. A procedure may be manual or automated. It is not simply a statement of what should be done, nor does it simply state what the organization wants to achieve. An internal control

is specific and should indicate the subject, object, action and when it is to be performed. Although a control often carries the word "ensure", that word is not enough. The objective of a control is to ensure that certain risk is mitigated. A statement containing only the "ensure" clause is a control objective, not the actual control. A control must be action oriented, not just objective oriented. A key word in the above definition is "established". This means that the control must be sustainable, it is not an hoc action or something a manager wants to do but other like managers are not required to do. "Established" also means it is required, specific, consistent and enforceable. An internal control deficiency is not simply an undesirable occurrence. Rather, it is a lack of control or a failure in internal control compliance. For example, a system administrator forgetting to lock the server room door is not a control deficiency, it is an incident. The deficiency is what would allow this to recur regularly, e.g., no explicit instruction or system enforcement of door locking. A recommendation to mitigate this is not simply to remind people to lock doors or "lock the door next time". A recommendation has to be a sustainable, established control.

Strictly speaking, an internal control is not an essential activity to carry out a transaction. However, a transaction without internal control is risky. For example, identifying a customer in an ATM transaction is not an internal control even though "identification" is commonly included by security specialists when designing the "identification, authentication and authorization" model. The ATM has to identify the customer in order to pull up the account information, so identification is an essential activity. Authentication is a control because strictly speaking, a bank can choose not to use authentication. Without authentication, identification is subject to higher risk.

Internal controls should not be a separate set of system functions or procedures. Instead, to ensure that internal controls are carried out consistently with management ownership, management should integrate internal controls in systems and operation procedures. Some controls of a policy nature may be published and communicated on a standalone basis, e.g., a code of business conduct. In addition to forming part of a system's computerized functions and operation procedures, internal controls should be compiled in a separate document, e.g., an internal control manual. This separate compilation is performed to help management to continuously assess risks and get their fingers around what controls are in place in the organization. Internal control objectives should be included in this compilation to help people understand the purpose of the controls. Management can use the internal control manual to organize, coordinate and correlate internal controls to provide sufficient redundancy to prevent risks from being ignored while avoiding significant duplication of effort. Such correlation is called a plan of internal controls. This plan should be documented and used as a basis for employee training.

Risk always exists. For example, it could rain on any day. But a reasonable person would not carry an umbrella every day. So when is an internal control necessary? It is important to keep in mind that internal controls should be enough to provide reasonable assurance that material risk does not remain. The key words are "reasonable" and "material". For example, I don't have to give much thought to cost effectiveness or whether a favorite

chocolate bar has passed the "best before" date by a week if it goes on sale for 25 cents each. That's materiality. "Reasonableness" means the cost of the control must not exceed the amount of risk being mitigated. It also means that the control is not too onerous and is user friendly. A control that is not user friendly, no matter how appealing it is on paper, will run a high risk of non-compliance.

Employees should be trained on internal controls and understand the objectives. This will help ensure compliance. Here is a story that shows the importance of training and understanding objectives.

A computer equipment manufacturer prides itself on communicating its strategies so that every employee is aware of the company goals. An auditor decided to test this claim. She asked a summer student sweeping the factory loading dock how his job related to company goals. The summer student replied as follows.

"My company's goal is to reduce the cost of its products. A major cost is inventory. We recently shifted to just-in-time production to reduce inventory stocking cost. This means our suppliers deliver products to us every two hours. If I don't clean the loading dock before the next load arrives, we are unable to accept delivery. This would set back the production schedule in the plant and increase the cost of production. We would also have the added cost of returning the material to the supplier."

This young man is now the company's chief financial officer.

It is the responsibility of the system owner to design and implement internal controls. S/he of course will have to rely on technical staff. For internal controls that apply to the infrastructure instead of a specific transaction processing system, the executive responsible for the infrastructure is responsible for designing and implementing internal controls, i.e., the CIO. The executive responsible for internal controls is also responsible for communicating internal controls to people and monitoring for compliance.

Compliance monitoring can take the following measures:

- Surveying employees.
- Meeting with unit managers.
- Transaction walkthrough, taking one or two transactions to test system and manual controls.
- Monitoring control, i.e., controls over controls e.g., management review of logs.

Compliance monitoring must be structured and disciplined. The chief risk officer should set up a process for compliance monitoring by system owners. This should be a requirement stated in the risk management policy.

COBIT Definition of Internal Control

Information Systems Audit and Control Association has developed Control Objectives for Information and Related Technology (COBIT). COBIT's definition of internal control is:
"The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."

According to COBIT, IT processes fall into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. These domains consist of 32 processes facilitated by the following 5 classes of IT resources: data, application systems, technology, facilities and people. COBIT identifies 271 control objectives.

REGULATORY REQUIREMENTS ON INTERNAL CONTROLS

Organizations should be aware of the relevant legislation, regulation, and business practices in the countries in which they do business – in order to assess the organizational impacts and requirements. The United States Sarbanes-Oxley Act of 2002 (SOX) requires public companies to report on internal controls annually along with their financial statements to Securities Exchange Commission. Canada's Investor Confidence Rules contain a similar provision. Regulators of the financial services and energy industries also have smaller scale requirements for internal control reporting.

Sarbanes-Oxley Act

The Sarbanes-Oxley (SOX) Act was intended to reform public accounting practices and other corporate governance processes and shore up the capital markets in the wake of the Enron, WorldCom, and other corporate governance scandals. Although SOX does not specifically address the issue of IT controls, this does not mean IT can be ignored when performing the compliance reviews required by the Act. The Act is neutral with regard to technology, but the implication is clear that IT controls are critical to the organization's overall system of internal controls. IT controls address the secure, stable, and reliable performance of hardware, software, and personnel to ensure reliability of financial applications, processes, and reporting, they are significant elements of internal controls in any public company.

Some key IT control areas have been interpreted as not included in SOX compliance. These include disaster recovery planning, privacy policy as well as business continuity and business planning systems. The following is a brief description of the relevant sections of SOX related to auditors and IT Controls.

Sections 103 and 802

These sections establish rules for public accounting firms related to the audit of financial statements. They also require that the auditors test the internal control structures and attest to the strength of those structures. This must include a thorough examination of the IT controls that are fundamental to the system of internal control over financial reporting.

One specific requirement relates to the retention of records "that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets…" Again, this is strongly influenced by the way in which IT records are maintained and retained.

Sections 302 and 404

Section 302 of the act requires the chief executive officer (CEO) and the chief financial officer (CFO) to evaluate the system of internal controls and report their conclusions and any changes in controls.

They must disclose:

- "all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls";
- "any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls".

Section 404 requires that the CEO and CFO must produce an annual audit report that:

- assesses the effectiveness of the internal control structure over financial reporting,
- discloses all known internal control weaknesses, and
- discloses all known frauds.

This will cover all applicable IT controls including software change controls and application controls.

Investor Confidence Rules

Canadian Securities Administrators (CSA) has adopted the Investor Confidence Rules that require the CEO of a public company to certify internal controls to its provincial securities commission every year. The provisions are similar to those in SOX. CSA is an umbrella organization of Canada's provincial and territorial securities regulators whose objective is to improve, coordinate and harmonize regulation of the Canadian capital markets.

INTERNAL CONTROL CLASSIFICATIONS

There are two ways to classify internal controls. One is to classify them by function. The other way is to classify them by scope. By function, a control can be preventive, detective or corrective. By scope, a control can be general or application specific.

It is quite obvious that preventive controls are more effective than detective or corrective controls. However, there is a limit to which an organization can implement preventive controls before making the environment inflexible and difficult to operate. Further, preventive controls can break down because of system malfunction or human circumvention. Detective controls, which are less intrusive, are needed. When a problem is detected, corrective measures will have to be taken. Management should implement preventive controls to a point where the cost of additional preventive controls would outweigh the benefit. The remaining risk will still very likely be significant. To mitigate the remaining risk, management should implement detective and corrective controls.

In addition to preventing, detecting and correcting mistakes, controls are also needed to monitor other controls, i.e., to check if other controls are being complied with. For example, a system control to report on delinquent management approval of electronic timesheets is a control over control and it mitigates control risk instead of inherent risk. Another example is management review of bank reconciliations.

Controls can vary in scope. A control that applies to the entire organization is generally desired because it ensures standardization. However, such a control can make operation inflexible and ineffective where business units are exposed to different degrees of risks and a variety of systems are used. Thus, controls specific to environments and applications are also needed. Organizations should adopt a combination of general controls that apply to multiple systems and application controls that apply to specific systems. Both general controls and application controls can fulfill the functions of prevention, detection and correction. General controls should be designed and implemented first. Application controls should then be designed and implemented for each system.

In Chapter One, we discussed the five components of a system as procedures, infrastructure, software, people and information. Internal controls are needed to address all of these components. Internal controls can take the form of procedures, infrastructure, software and people. Procedures include policies, standards and operation procedures.

Internal controls, whether general or application, start at the policy level. Procedures are instructions for users to interface with a system and interpret system information. Procedures are based on policies, which contain mandatory statements about governance, expected behavior and adopted principles. Policies are less fluid than procedures as the latter are used to guide day to day operation. Procedures are written to comply with policies. Because procedures are for people to use, they do not apply to automated functions. How do automated functions comply with policies? Such compliance is achieved in two ways. First, policy requirements should be included in systems development user requirements and design specifications that we will discuss in the next chapter. The extent of such compliance, however, is often questionable. For example, how long should a password be? To address this, standards can be created. Standards sit between policies and procedures. They also sit between policies and system specifications. Standards are changed more frequently than policies and less frequently than procedures.

GENERAL CONTROLS

General controls can be classified as follows:

- Organization controls
- Software change controls
- Access controls
- Systems development controls
- Disaster prevention and recovery controls
- Technology infrastructure controls
- IT performance measurement controls
- Intellectual property controls

ORGANIZATION CONTROLS

We trained hard…but every time we formed teams we would be reorganized. I was to learn that we meet any new situation by reorganizing. And a wonderful method it can be for creating the illusion of progress while producing confusion, inefficiency and demoralization.

Petronius Arbiter, Roman writer and satirist, 210 B. C.

Here is an old joke about management:

A new executive reports for work and is shown to his office. On his desk is a letter from his predecessor and three sealed envelopes numbered 1 to 3, labelled "for future reference, not urgent". The letter congratulates him on his new position, the former executive regretting he was unable to stick around and help with the transition. The new executive tosses the 3 envelopes in a drawer.

Months go by and the executive is faced with a problem that seems unsolvable. He recalls the three envelopes. Frustrated and desperate about the problem, he opens the first envelope. He finds a note that says "blame everything on me." The executive calls in his direct reports and declares that all the problems they are facing are due to his predecessor and that the division will now turn in a new direction.

A few months later, the next big problem emerges. The executive finally brings himself to open the second envelope. The message inside reads "reorganize everything." He then calls a meeting and declares that the current situation is the result of poor organization and that the entire division must be restructured. It is a very busy time and everyone is occupied with the rigor of reorganization for months and months.

Shortly after, the next problem presents itself to the executive. He then opens the third envelope. The message says "fill out three new envelopes".

Sometimes, the problems faced by executives must be addressed head-on, without looking to place the blame or just reorganization. The following organizational control practices should help a CIO to avoid the above situations.

The objective of organization controls is to ensure that operations involving I & IT follow best practices that are consistent throughout the organization and compatible with customer and stakeholder expectations. Controls in this category include:

- An I & IT strategy that is congruent with the business strategy.
- A governance structure including a process to keep the board of directors informed of IT direction and major IT projects .
- An IT steering committee that oversees IT investments and provides IT direction.
- An audit committee made up of independent directors that provides oversight on internal audit coverage, external auditor selection as well as management actions to remedy control weaknesses and transaction irregularities. These functions include:
  - Approving the annual internal audit plan.
  - Approving the annual appointment of the financial statement auditors.
  - Reviewing periodic reports on internal audit findings and holding management to correcting the deficiencies and mistakes.
  - Reviewing the annual shareholders' auditors report.
  - Reviewing the annual shareholders' auditors' management letter on internal control recommendations.
- Policies and procedures that address:
  - The responsibilities for IT investment, deployment, monitoring and controls.
  - The approval levels for IT investments.
  - IT risk assessment and acceptance, we discussed this in the last chapter.
  - Systems development, we will discuss this in the next chapter.
  - Procurement of IT products and services.
  - Hiring, including requirements for job posting, interviews, tests, reference checks and criminal record checks (for sensitive positions).
  - Staff development, including mandatory training plans, analysis and reporting of training achieved in relation to job descriptions. Organizations should also encourage and financially support professional memberships that are relevant to employees' responsibilities and help employees keep up with professional development.
  - Privacy, we will discuss this in Chapter Five.
  - Security, we will discuss this in Chapter Eight and Chapter Nine.
  - Technology infrastructures.
  - Capacity planning.
- Organization charts and job description to cover every IT employee.
- A defined reporting relationship between the chief information officer (CIO) and a senior executive, who should be the chief executive officer or the chief operating officer (COO). If the CIO reports to other executives, the arrangement can make the CIO's role less effective as it sends the message that the organization does not view IT as top corporate priority. For example, if the CIO reports to the chief financial officer, the IT department may receive undue influence in devoting its resources to support financial systems. A similar problem would occur if the CIO reports to a line executive. Organizations that have CIOs reporting to lower levels than the COO will find it hard to attract top calibre people to fill that role.
- A designated executive accountable for information security.

- Segregation of duties between the IT department and business areas to support a process for independent approval and review of IT expenditure, facilitate the detection of errors, and prevent frauds and improper practices.
- Segregation of duties within the IT department to provide for independent approval and review, facilitate detection of errors and prevent frauds and improper practices. This may be less practical in small organizations, where heavier reliance will have to be placed on application controls to compensate.
- Procedures for hiring consultants to ensure value for money, proper approval and knowledge transfer to staff.
- Staff development procedures and a performance review process to ensure the organization continues to have high quality of IT staff.
- IT budget review procedures.
- Procedures for accounting and cross-charging IT expenditures. This deters unnecessary use of IT and holds managers accountable for effective IT deployment. The cross-charge rates must be competitive. It would be discomforting and counter-productive if the cross-charge rates are higher than market rates.
- Systems and procedures for IT asset and information inventory control.
- A skills database indicating who have the skills for each position in the organization. There should be enough redundancy built in.

I & IT Strategy

The board of directors should challenge management to develop an I & IT strategy that is congruent with the business strategy. The I & IT strategy should describe the direction of the IT environment in the organization over the time frame of the business strategy. The following information should be included:

- A description of the organization's dependence on IT to sustain and grow its business and operation. This will also entail how competitors are using IT. The criticality of IT in each business line should be assessed.
- The approach to managing the investment in and operation of IT. Will there be significant dependence on software and hardware vendors and how will this affect the organization's competitiveness?
- The organization structure for managing the IT investments and information systems.
- The staffing plan for managing and operating information systems. This should include projected attrition and a strategy for succession planning and staff development to ensure that the organization has competent human resources to develop, maintain and operate information systems.
- The cost and justification for annual IT investments including the maintenance of current IT assets and operations.

- IT infrastructure development plan.
- Systems development plan. We will talk more about this in the next chapter.
- eBusiness plan. No organization is immune to the Internet's influence. Most of them cannot compete without offering electronic business services. This global network enables big companies to act small and small companies to act big. For example, multi-nationals can use the Internet to reach individual customers anywhere in the world and use electronic business activities to study the pattern and preferences of retail customers in order to give them tailored attention. Small companies can similarly use the Internet to reach large corporate clients and do business with them.

IT Governance

IT governance is part of corporate governance. While it is clear that the board of directors, the CEO and the COO are directly accountable for corporate governance, it is less obvious as to who are accountable for IT governance. Should it be the CEO or the CIO? IT governance is about making sure that IT is used effectively to support the organization. The same parties accountable for corporate governance are also accountable for IT governance. In addition, the CIO is accountable.

AICPA defines IT governance as follows.

IT governance is a framework that ensures that technology decisions are made in support of the business' goals and objectives. IT governance is the responsibility of the board of directors and executive management. It is derived from corporate governance and is concerned primarily with the connection between business focus and IT management of an organization. The primary goal for IT governance is to assure that the investments in IT generate business value and the mitigation of risks associated with IT.

A steady influx of business regulations is forcing companies to find new strategies that minimize the burdens and maximize the benefits of addressing regulatory compliance. Companies can obtain a range of benefits from regulatory compliance, including more accurate financial reporting, improved visibility of risk, and better IT governance. IT governance is part of corporate governance and it provides the organizational structures to enable the creation of business value within information technology (IT). Part of this process is obtaining assurance that IT investments are only made in beneficial projects and that there are adequate IT control mechanisms. By aligning IT planning with organizational goals, IT becomes a key player in evaluating the business issues that factor into enterprise-wide decision making. Standardized frameworks for IT governance and accounting controls are among the tools available to companies that can be used to link Sarbanes-Oxley documentation activities with corporate IT management procedures. This resource area will provide you with the information and tools to meet the numerous challenges of IT governance and regulation.

Source:
http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/ITGOVERNANCE/Pages/default.aspx, accessed on February 19, 2014.

IT governance includes mainly a framework to ensure that the right technology is used and technology is used right. This framework is made up of organization charts, staff, policies, standards, corporate procedures (as opposed to local procedures), training and monitoring systems. IT governance is of an assurance and monitoring nature, to assure the board of directors that the organization's IT adequately supports the organization's business. It is not the same as the IT infrastructure, which is needed for day to day operations. In other words, if IT governance breaks for a day, business will still be as usual. But if it is absent for a month or a few months, the organization's competitiveness and survival will be in increasing doubt.

The CIO needs support from other executives in carrying out IT governance. Such support should be lent on a frequent basis formally and informally. An effective and common formal support mechanism is an IT steering committee. This should consist of the C-suite of executives and the heads of major business lines. For example, the IT steering committee of a major Canadian bank consists of the CEO, COO, CIO, CFO, chief administrative officer, the treasurer as well as the heads of personal banking and commercial banking, corporate and government banking, and international banking. The mandate of this committee is to set the IT strategy, approve major IT projects, monitor major IT projects, make major IT risk decisions and provide ongoing senior level guidance in IT risk management.

Responsibility of the Board of Directors

The board is expected by shareholders to set business direction for the organization and monitor operation to ensure that it is in line with the stated direction. Monitoring is performed by means of reviewing information provided by management. Most organizations have board committees to focus on specific areas of corporate significance. Some committees are required by regulations, e.g., the audit committee is usually a requirement of the securities regulator, the industry regulator or legislation for incorporation. Typical committees are audit, compensation, corporate governance as well as health and safety. Why isn't there an IT committee?

The board looks at IT as a means of doing business, e.g., to make business more efficient. Some boards of large companies that have corporate governance committees use them to address IT governance. Some IT companies indeed have technology committees, and this is a favorable trend for all public companies, to show more transparency to shareholders that the companies will continuously review the use of IT to be more competitive. The IT steering committee made up of senior executives should make sure the board is informed of major IT risks, the IT strategy and progress in delivering the strategy.

Segregation of Duties

Employees that can perform a variety of duties are valuable to the organization. However, in reality, there are few, or no supermen and superwomen. Thus, after a certain point, the more different tasks an employee performs, the less good s/he is on any of them. It is important to limit the types of work an employee performs. Such limitation serves the purpose of building expertise and efficiency, as well as preventing mistakes and fraud. It is also important to cross train employees and expand their horizon. Segregation of duties does not work against that. Employees can be cross trained under supervision to build their knowledge in other areas but they don't have to be given the access to information or charged with the expectation to do work in multiple areas regularly. Segregation of duties supports the control criteria of accuracy, authorization, occurrence and efficiency.

The purpose of segregating duties is to provide opportunities for errors to be detected and to reduce the opportunity for irregular practices or fraud. Incompatible duties should be separated. Two functions are incompatible if they satisfy the following criteria:

- Having one person performing both functions will unduly and significantly increase the risk of fraud or undetected errors.
- Assigning the functions to at least two persons will not significantly impair operation effectiveness or efficiency.

Segregation of duties is therefore based on risk assessment. Where it is impractical to segregate duties because of staff constraint, an organization can mitigate the resultant risk with more rigorous exception reporting and management review.

Segregating IT from Other Functions

The IT department should be separated from business units and other corporate functions. Simply stated, the CIO should have no other responsibilities and IT people should report to the CIO but not to the business units or other corporate functions. The purpose of this segregation is threefold.

First, this allows IT people to focus on IT, which is a specialized area that calls for frequent knowledge upgrade. Letting IT people work on non-IT areas or projects would distract their focus. Similarly, business units and other corporate areas need to develop their own expertise that is not directly related to IT. They view information technology as a set of tools and this is the right attitude. If IT people were to run the business or accounting, there is a danger of letting the tools drive the business instead of the right approach of letting business requirements determine the tools.

Secondly, IT should be separated from the business and other corporate functions in order to establish proper accountability. If IT performs other functions, it would be easier for the users of those other functions to "blame it on the system" when something goes

wrong. Business units and corporate executives should take ownership of their functions and results. They should determine how much information technology to use and how many internal controls to implement, instead of letting IT decide.

Thirdly, organizations should distribute functions to avoid one party having extensive control over transaction processing. The information technology department has full control over information and significant damage can result from mistakes or rouge behavior. Organizations should not add to this risk by giving IT people the responsibility for initiating accounting entries or business transactions. By separating this from IT, there is more assurance that system information is adequately supported by legitimate business transactions and accounting decisions.

Segregation of Information Technology Functions

For the same reasons as above, IT functions should be segregated to the extent practical. Obviously, segregation of duties has to stop somewhere, otherwise the organization will become extremely bureaucratic and people will spend more time communicating and seeking approval than actually doing the work. Research as well as industry experience in IT effectiveness and reliability indicate that systems development and technology infrastructures should be separated. In addition to helping people focus, this separation would mitigate the risks of:

- systems developers implementing software without approval,
- systems developers changing business information and
- technology infrastructures people developing systems without approval.

In other words, separating systems development from technology infrastructure prevents improper changes to systems and information. Within systems development, the following functions should be further separated to facilitate expertise development and prevent improper activities:

- Systems analysis (business interfaces)
- Systems architecture development
- Systems design
- Programming
- Testing
- Quality assurance
- Project management office

These functions are described in more detail in the next chapter.

Similarly, the technology infrastructure function can be further separated as follows:

- Server administration
- Network administration
- Desktop administration
- Database administration
- Disaster recovery planning and maintenance

- Capacity planning
- IT research
- Information security

The first three functions above are performed by system administrators. This position requires full access to the assigned servers or desktops so hiring must be subject to close scrutiny and background check. A system administrator installs and configures the operating system, installs applications based on management authorization, creates, modify and delete user accounts based on management authorization, installs system software like anti-virus, monitors and troubleshoots server performance. To give you a perspective of the significance of this function, you should know that Edward Snowden was a system administrator in United States National Security Agency. A system administrator must not perform any other IT functions because this job's system access is already powerful enough to lead to the materialization of significant risks, so management should not widen the potential for errors or fraud. Management should implement operating system log analysis software that generates reports for managers' review based on instructions and such review should be tracked by the reporting software to make sure it is done.

Database administration is in charge of configuring and maintaining the database management system. This function must be independent of server and desktop administration for segregation of duties. A database administrator (DBA) has similar functions to a system administrator but the object of control and monitoring is the database management system. A DBA also maintains the data dictionary (described in chapter 4 and chapter 6), creates, change and delete access profiles for applications and users based on management authorization. Most users access database tables via applications. However, in certain cases like special projects, a user may be granted a database management system user ID to access database tables directly for data analysis using data mining tools, Excel or Microsoft Access. Database logs should be subject to reporting and management review like server logs.

In large organizations, the following functions should be moved out of the systems development and technology infrastructures areas to provide better focus and reduce the exposure to undue or biased influence from systems development and technology infrastructures. These functions should report directly to the CIO.

- Information security
- IT research
- Quality assurance
- Project management office

If information security reports to the executive in charge of technology infrastructures, it may not receive adequate emphasis. When there is a crunch or financial pressure, technology infrastructures may sacrifice security in favor of efficiency; and that can present an unacceptable risk to the organization. By aligning the information security function to report to the CIO, there is more assurance that information security will receive adequate emphasis in the organization.

Organizations need to keep up its competitiveness by using the right technology. Focused effort and a high degree of expertise are needed. An increasing number of organizations have established the position of chief technology officer reporting to the CIO to focus the effort of IT research and assessment.

The purpose of quality assurance is to ensure systems reliability by developing policies and standards, training IT people and performing independent testing before implementation. This is not to be confused with the assurance responsibilities of line executives and internal audit. Line executives should carry out periodic risk assessment of their own systems currently used in transaction processing. Internal audit tests and assesses systems periodically to provide independent control assurance. The main reason for the quality assurance function is to ensure that new systems are developed and implemented properly. In addition, this unit should be responsible for developing IT policies and procedures. Because of the somewhat independent nature of this function, i.e., independent of system design and programming, it should report directly to the CIO.

The role of the project management office is to monitor IT projects to ensure timely and proper completion. Proper completion includes completion on target and budget. Because of the monitoring role of this function, it should report to the CIO.

In a large Canadian bank, the executive vice-president and CIO has the following direct reports:

- Senior vice-president of systems development
- Senior vice-president of technology infrastructures
- Vice-president and chief information security officer
- Vice-president and chief technology officer
- Director of quality assurance
- Director of project management office

The chief technology officer (CTO) title is increasingly common in large organizations. This person is often viewed as the “technical CIO”. S/he is actually the technical advisor to the CIO. This job serves to ensure that the organization uses the right IT, i.e., using modern IT to support the business effectively. Effective use also includes consistency and scalability across the organization. The CTO has a staff of technical IT specialists who perform research and beta testing.

Segregation of duties should be implemented using organization charts, job descriptions, procedures and access control.

Code of Business Conduct

Every organization should have a code of business conduct that instructs employees about what is acceptable and what is not acceptable in their dealings with customers, colleagues and other external parties. The code should also tell employees what is not acceptable in using organization resources such as email. We will discuss the relevance to

IT resources in more detail in Chapter Eight and Chapter Eleven. Employees should be asked to acknowledge this code upon acceptance of a job offer and should be reminded periodically by means of email or a pop-up screen upon network logon.

Management of Consultants

IT consultants are commonly used to fill the gap between business requirements for IT support and available staff resources or expertise. Consultants are more fluid and expensive and therefore should be subject to rigorous justification to hire and close monitoring. They may not be as familiar with the organization's rules of dos and don'ts so may need more guidance than employees. Usually, an advantage they have over employees is their IT expertise. The following is a checklist that should be followed in hiring and managing consultants.

1. Follow the organization's procurement policy with respect to sending out requests for proposals. Establish a list of requirements and factors for assessing proposals to include technical requirements, reference checks, criminal record checks, desirable skills, knowledge and prices etc.
2. Inform the chosen and declined vendors in writing.
3. Obtain management signoff for the chosen vendor before the contract is signed.
4. Use the organization's standard contract which has been approved by the legal department. Add information about the assignment.
5. Require proof of malpractice and liability insurance.
6. Include a statement of work that details the deliverables in the contract.
7. Require the consulting company to sign the following agreements:
    - confidentiality agreement to keep the client's non-public information confidential during or after the engagement, unless otherwise directed by the client;
    - assignment of copyright, giving the client copyright to all material developed by the consulting company or the assigned consultants during the engagement;
    - waiver of moral rights, therefore giving the client the right to use the developed work in any way it sees fit without breaking the law and to alter the work;
    - an agreement that discloses all inventions during the term of the contract within the scope of the statement of work and that grants the ownership of invention to the client at no additional cost other than the consulting fee covered in the contract.
8. Approve invoices based on examination of deliverables rather than just time sheets.
9. Meet with the consultant frequently to monitor progress.
10. Document a performance appraisal at the end of the contract. If the contract goes beyond six months, an interim performance appraisal should be documented.

SOFTWARE CHANGE CONTROL

Changes are always risky. Even obviously favorable changes are risky. A salary increase may be calculated incorrectly thereby short changing employees or causing unnecessary payroll expense. If you win a lottery jackpot, you will be riskier in the short term. You will be at a higher risk of being robbed and your driving may be less focused while your mind wanders to world wide travel. Change management is the process of mitigating the risk of changes.

Software changes are made from time to time, even for new systems. This is because no matter how much a system has been tested before implementation, there will be bugs discovered during operation, and the bugs require correction. Another reason is that business requirements change from time to time. Software changes need to be managed with approval, documentation, cost justification, testing and conversion. There also have to be controls to prevent unauthorized changes.

Internal controls are needed to ensure that software changes are implemented:
- only based on written management requests,
- completely,
- accurately,
- with authorization,
- on a timely basis, and
- efficiently.

Software change controls should include the following:
- Software change control policy and procedures
- Testing procedures
- Software library controls
- Software change tracking
- Code (program) comparison

Software Change Management Policy and Procedures

Almost all internal controls start with policies and procedures. Management states the control objectives and accountabilities in policies. Procedures tell people what controls to carry out, how and who should carry them out.

Every organization should have a software change policy. This policy will define who are authorized to request and approve changes. It will also set thresholds for approval in terms of the amount of human, software and hardware resources required to design and implement the change. In other words, every change request should be accompanied with a business case, no matter how simple the change is. A change request should state the benefit, quantifiable where practical, of the change. Requests should be generated by user

area management and approved based on a schedule of signing authorities depending on the magnitude of the change in terms of resources required. The change management policy and procedures should address the following:

- Definition of what constitutes a software change. Basically, this means any change to a computer program.
- Criteria for estimating the magnitude of the change, e.g., in terms of person days and human resources cost required to complete the change. Also, software and hardware resources should be estimated.
- A change request form that states the identity and rank of the requester, the identity and rank of the approver and the project manager for the change. No matter how small a change is, it should be assigned to a project manager who will likely manage a number of small projects concurrently. The project manager can be assigned by the requester, the approver or the CIO department. The required delivery date should also be specified. In organizations that cross charge IT cost, the cost center of the requester should be stated. Every change request should be a project or part of a project to enable tracking and ensure compliance with the software change policy and procedures.
- Criteria for justifying a change request based on cost and benefit.
- Criteria for ranking and approving change requests.
- Types of testing required and the responsibilities. Many large organizations use a change control board made up of IT management and a cross-section of managers from the organization. This board is similar in composition to the IT steering committee but at a lower level. Its mandate is to review and approve changes. There should be criteria for referring change requests to this board and criteria for the board to use to approve. The criteria should include the cost and benefit of the change, impact on current systems and the risk of the change. Risk assessment of a change request should be made in accordance with the organization's risk assessment and acceptance policy that we discussed in the last chapter.
- Naming conventions for programs, e.g., if this is 101st program in the system, how is it numbered and named?
- Stages of approval and approvers.
- List of approvers.
- Criteria for and extent of system testing.
- Separation of development, testing and production (operation) libraries. A library is a collection, like a folder, of programs.
- Tracking of source and object code (programs).
- Tracking of change requests.
- Forms and related documentation for closing a change request.

Software Library Controls

A software library is a collection of computer programs for a system. It is like a folder of files, except that the files are computer programs. It is not the same as the system itself, which consists of an integrated set of computer programs that have been compiled and

linked and is fully operational. The purpose of a library is to keep track of the versions of computer programs during development and in operation. A library consists of the source code and object code to keep track of completeness and facilitate changes.
Access to system libraries should be restricted. Large organizations should use automated tools to track and control program movement during development, testing and implementation. Such a tool is commonly called a software change management system.

Source Code, Object Code and Executable Code

The word "code" is commonly used to collectively refer to computer programs. A program in the form of the chosen programming language is called source code. Source code is understandable to programmers but not the operating system. For computer programs to be operable, they must be translated to computer languages (machine languages). A program translated to a computer language is called object code. This translation process is called compilation. Compilation is an automated process. Once a programmer highlights the source programs and clicks "compile", the programs will be compiled object code. Before translating source code to object code, a compiler checks the syntax (grammar) of the source code programs. Each programming language has its own syntax requirements.

A source code instruction (a line of code) is often compiled to several lines in object code. This is because a programmer does not have to worry about how hardware resource like real memory is allocated and how to keep track of real time calculation and intermediary results in RAM and the central processing unit (CPU). Object code also includes the standard CPU hardware instructions carried out to satisfy a source code instruction, e.g., how to compare data, how to divide two numbers. At the end of compilation, the lines of object code are usually linked to an executable code file, like a .exe file.

What is a computer language? It is the collection of terms including nouns and verbs that are understandable to the computer's operating system. The operating system (e.g., Windows) in turn interacts with the central processing unit (CPU, the computer's brain) and peripheral devices like input, storage, output and memory. In the 1940's and 1950's, computer programs were often written in computer (machine) languages. Programmers had to understand the operation of the CPU and peripheral in order to program and a program could take days to write. As computers became more powerful and programs grew in functionality and length, it became inefficient for programmers to write programs in computer languages. Programming languages of a more narrative nature like PL/1, BASIC and Common Business Oriented Language (COBOL) were invented to make programming more user oriented and efficient. However, even today, software that interacts directly with the CPU like an operating system and electronic circuit control functions still has to be written in computer (machine) languages. Many legacy systems in current use were developed using COBOL and PL/1 (especially in financial institutions). BASIC is a simpler language for small systems. It uses an interpreter instead of a compiler. An interpreter is a just-in-time compiler. Instead of producing objective

code and linking to executive code, an interpreter interprets source code instructions when the program is run on the operating system, at which time object code is produced. This makes system development more expedient but increases the transaction processing time so it is suitable for small systems, also suitable for systems that change more frequently like web based systems.

Common modern programming languages include PHP, C, Java and Javascript. PHP is an open-source, interpretive, server-side, cross-platform, HTML scripting language, especially well-suited for Web development as it can be embedded into HTML pages. Open source means it is free for download. HTML (hyper text markup language) is the original web page standard for presenting static data via a URL link. C is a general-purpose programming language that is also the basis for its faster scripting children, C++ and C#. Java is used is the back end (server side) of many popular web sites including Facebook, Google and Twitter. Javacsript is even more popular and is the predominant language for front end processing in many popular web sites. Javascript is a distant cousin of Java in that both are object oriented programming languages with similar structure. But Java contains a much larger set of instructions. Java programs require a compiler whereas Javascript is mainly an interpreter programming language. Javascript is lighter and faster so it is predominantly used in front end processing where devices have lower computing power than servers.

Object oriented programming means writing programs for common functions in modules instead of writing programs in accordance with the chronological processing steps of a system. The common functions are grouped by classes, e.g., calculation vs comparing values. This allows programs to be more portable for updates and transfer between systems.

A program written to run on a Mac computer can quite easily be modified to run in Windows by recompiling it using a Windows compiler for that programming language. However, a program in object code for a Mac computer cannot be run on a personal computer because of the different architectures of these computers.

Most programming languages allow programmers to write comments or explanatory notes about program instructions to make a program easy to follow by programmers. Such comments or notes are ignored by the compiler or interpreter.

Programmers' Personal Library (program writing and programmer's own testing)

When a programmer is assigned a change request, s/he needs the current version of the programs to be changed or interfaced. S/he can go fetch the programs directly or obtain them through a change control coordinator. The change control coordinator is part of the quality assurance department described earlier in this chapter. In a large organization, there may be several change control coordinators who are assigned responsibilities for different business areas. The latter is a more desirable approach as it ensures proper segregation of duties. The programmer then makes the changes and writes new programs. While s/he is doing that, no one should have access to the "work-in-progress". Such work-in-progress should be in the programmer's own library. In this library, the

programmer will also conduct testing. When a programmer is satisfied that the programs work, s/he will ask the programming manager to review and approve. It is impractical for the programming manager to review all the programs. In practice, the manager will peruse the programming documentation (narrative description in the form of comments instead of the actual program steps) and review selected and critical code. To supplement his or her limited review, the programming manager usually asks other programmers to review the code and conduct peer testing. Each programmer should have full access to his or her own library and read access to a common development library.

Development Library (peer testing or string testing)

When the programs undergo peer review and testing, they should be located in the development library. Every programmer in the group can have read access to this library but only the change control coordinator should have write access. When programs are ready for peer review and testing, the programming manager will inform the change control coordinator who will then take the programs from the programmers' personal libraries and put them in the development library. The actual fetch and deposit of programs will likely be via the software change management system. The peer testing should use more data and be more rigorous. It is also called string testing because a string of programs is tested together including their interfaces.

Only the change control coordinator should have the access right to move programs into the development library. No one else should have update access to the programs. What happens if the peer testing identifies program flaws? The programming manager will be notified and the programs will be returned to the authors or reassigned to other programmers to fix. In either case, the programs will be transferred to a programmer's personal library via the software change management system.

System Integration Test Library (system integration testing)

Once the programs have passed peer testing, they should be subjected to more rigorous testing in an integrated manner. This means testing the programs along with the rest of the system or major module and including even the programs that have not been changed. This is called system integration testing (SIT). It is the change control coordinator's job to move the programs from the development library and the related but unchanged programs from the production library to the test library. In large organizations, there may be different coordinators that control different libraries, e.g., one coordinator controlling the development library and another coordinator controlling the test library. We will discuss production library a little later. Integration testing is more rigorous than peer programmer testing because it includes interfaces with the entire system or module. A module is a major section of a system consisting of a lot of functions. Whether the entire system has to be tested or only certain modules are tested depends on the extent of programs being changed. The criteria should be stated in the change control procedures.

Only the change control coordinator should have the access right to move programs into the test library. No one else should have update access to the programs. There should be backup change control coordinators.

Who should perform integration testing? These testers should not be programmers in order to maintain objectivity. They should be dedicated testers. Their background does not have to be in IT. In fact, some large organizations have hired liberal arts graduates or transferred business unit employees to be testers. A tester has to be meticulous and good in documentation. The former CEO of a major North American bank was a system tester after he graduated with a degree in history. Testers have no access to source code and have only the access right to run executive code.

What happens when program flaws are revealed in system integration testing? The programming manager is informed and the programs are sent back to the authors or reassigned to be fixed. The programs then have to go through programmers' own testing and peer testing before returning to the test library for system integration testing. In other words, a flawed program has to go back to square one instead of being corrected midway in the process (which is dangerous because the correction will then tend to be haphazard).

Where do the change control coordinators work? They are part of the Quality Assurance area.

User Acceptance Test Library

After system integration testing, the system changes are subjected to user acceptance testing (UAT). The testers are user representatives. This is the last phase of the iterative test cycle. It is a little less time consuming and extensive than system integration testing because at this stage, the system changes have been tested exhaustively in terms of reliability. UAT will repeat the functional tests in a smaller scale, e.g., using less extensive test data. In addition, it will include testing for system performance efficiency, user friendliness as well as comprehensiveness of the system reports and user procedures.

Only the change control coordinator should have the access right to move programs into the UAT library. No one else should have update access to the programs. What happens when program flaws are revealed in UAT? The programming manager should be notified and the programs are sent back to the authors or reassigned to be fixed. The programs then have to go through programmers' own testing, peer testing and SIT before returning to UAT. Testers have no access to source code and have only the access right to run object code but not to update object code.

Production Library

Once programs are signed off by users as having passed UAT, they are ready for implementation. A change control coordinator will move these programs from UAT to the production library. No one else should have update access to the production library. The production library consists of programs that are used in transaction processing, i.e., live programs. Because of the importance of the production library, movement into this library should require two change control coordinators, i.e., the change management system should require dual logon to implement any change. Even though this library contains programs used in transaction processing, it is offline. A copy of the approved and linked object code is moved to the transaction processing servers for live operation.

Movement of Source Code and Object Code?

A common question is whether the source code only or the object code only should be moved between libraries or both? Let's explore the pros and cons of these three options.

Option 1: Moving Source Code Only – This means that the source code has to be recompiled in the destination library because in order for the programs to be used for testing, they have to operate in a computer (machine) language.

Option 2: Moving the Object Code Only – There is no recompilation needed.

Option 3: Moving Both Object Code and Source Code – There is no recompilation needed.

On surface, option 1 seems to be the least desirable.

Even though source code, if everything goes well, is not needed in the common development, SIT and UAT libraries, it is needed in the production library. This is because when a programmer begins working on a changed request, s/he needs the current source code, which resides in the production library. The production library consists of programs that have been fully signed off and are working. This is the official version of the programs. Therefore, to maintain continuity and ensure completeness of transferring programs at each stage, source code should be moved between libraries throughout the cycle. Now option 2 does not look attractive. Further, when testing reveals a program bug, the software change management system will need the associated source code to tell the change control coordinator which source programs have to be fixed. So it is important to have source code in all libraries.

Option 3 moves the source code and object code between libraries. This introduces the risk of source code not compatible with object code because the wrong versions were moved. For example, the change control coordinator may have moved version 3 of object code but version 2 of source code. Moving is prone to losing things.

Under option 1, although only the source code is moved between libraries, object code can be created in each library by compiling from the source code. This ensures that object code is compatible with the source code. Option 1 seems to be the most desirable method to ensure synchronization between source code and object code. However, one would argue that if the wrong version of source code is moved, the compiled object code will be wrong. Well, let's adopt another option, option 4, which is the safest.

Option 4 – Move the source code and the object code to the next library. Once moved, recompile the source code and compare the compiled object code with the moved object code. This will make sure the correct versions of source code and object code have been moved.

Software Change Environments

For each library discussed above, there should be a hardware environment. The purpose of the environment is to hold the library and restrict access. In a large organization like a bank, an environment may be a data center. In smaller organizations, it may be local area network or even just a server.

Emergency Changes

Emergency system changes are inevitable. A common purpose is to fix a system problem to prevent or avoid prolonged outage. There is usually not enough time for the rigorous testing or documentation of testing normally performed. It is important that emergency changes be thoroughly tested after implementation and documentation should be brought up to date. To ensure that emergency changes are properly documented, tested and approved, the change management system should track these changes and report to the appropriate manager for actions. In fact, today's change management systems should automate documentation in terms of version control and audit trail as much as possible and prevent alteration or deletion of the audit trail. It should also send automated notifications to management and the quality assurance department. Emergency changes should require a special ID to implement and there should be automated reporting to management to check the adequacy of subsequent documentation and testing. The use of this ID must be highly restricted which requires a different password for each use.

Source Code and Object Code Comparison

Periodically, IT management should use software tools to compare the current source code with the backup or with yesterday's source code to identify changes. Changes should then be reconciled to the approval audit trail. Both source code and object code can be compared between versions. Source code comparison is more informative as it is easier to for programmers to identify the changes. Object code comparison is more

reliable because object code is closer to executable code. If an organization does not have the source code, such as using SAP, an integrated accounting system purchased from a software vendor, it should still perform object code or executable code comparison.

ACCESS CONTROLS

Access controls are increasingly important as organizations expand their use of eBusiness and open their networks to business partners. Organizations need to secure access to the computing environments and specific systems. Access controls support software change controls and organizational controls such as segregation of duties because for example, without access controls, a programmer can install programs without approval. Access controls can be general in nature or specific to applications. Many techniques are equally applicable in a general scope and a specific environment, e.g., a password can restrict access to the general network, another password can be used to access the payroll system.

Physical Access Controls

In spite of the increasing use of technology in all organizations, basic physical security is still important. In fact, it is becoming more and more important as computing devices are smaller and can hold a growing quantity of data. Here are some examples of key physical access controls.

- A system to record access.
- Access cards
- Access control procedures for premises that house hardware or software.
- Biometrics for granting physical access
- Fire and flood protection.
- Locks for portable hardware.
- Mantraps
- Restricted zones within a building
- Security guards
- Unmarked data centers.
- Video surveillance for multiple levels of access restriction for sever rooms and data centers.

Information Access Controls

Here are some examples of key information access controls. Information access controls take the form of policies, procedures, independent review and software functions. The last category is also called logical access controls.

- An information security policy that defines accountability and responsibilities.
- A process for assessing the sensitivity of information and linking sensitivity to security tools.
- Security standards to address:
  - Appropriate use of information systems.
  - Confidentiality agreement with employees and contractors.
  - Cryptography
  - eBusiness
  - Email
  - Incident response.
  - Intrusion prevention and detection.
  - Investigation.
  - Privacy
  - Remote access.
  - Security check as part of hiring process.
  - Server and workstation administration.
  - System security updates.
  - User authentication including password controls.
  - Virus detection and removal.
  - Vulnerability assessment.
  - Wireless security.
- A repository of information owners which contains names and titles of designated owners of systems. There should be one owner of each system. The owner will decide who can have access to the system and information stored in the system.
- Procedures for:
  - access granting and disabling
  - access violation review
  - investigating anomalies.
- Access logs

General access controls are increasingly automated and these include:

- Anti-virus detection tools
- Encryption software
- Firewall to protect the organization's network from the Internet
- Intrusion detection system
- Intrusion prevention system
- Passwords
- Single sign on
- Two-factor authentication
- Virtual private network

SYSTEMS DEVELOPMENT AND ACQUISITION CONTROLS

Studies show that the average organization spends about half of its IT budget to acquire and develop systems. A large percentage of IT projects fail to be implemented or fail to deliver the promised benefit. Common reasons for project failures include the following:

- Lack of senior management attention and review
- Unclear user requirements
- Incorrect or inaccurate user requirements
- Incorrect design
- Inadequate testing
- Unrealistic business case that understates cost and overstates benefit
- Incorrect or incomplete conversion
- Inadequate infrastructure

To mitigate these risks, an organization should have a systems development methodology that includes criteria for initiating and approving IT projects, documentation and testing standards as well as requirements for checkpoints and signoffs. We will discuss this in more depth in the next chapter.

DISASTER PREVENTION CONTROLS

We experience or see mishaps almost every day. Earthquakes, tornados, floods, fires, "break and enter" and terrorist attacks are common occurrences. These events can damage buildings, offices, files, computers and information storage media. Some of these are not within the control of most organizations. For example, earthquakes and tornados are beyond business organizations and even some governments to predict, let alone controlling. However, incidents of a smaller scale can be controlled by organizations. Incidents such as fire, flood, "break and enter" or overheating are well within the capability of most organizations to prevent. Disaster prevention controls for these events include the following:

- Alarm systems.
- Close circuit TV and monitoring stations.
- Fire extinguishing devices.
- Hardware performance and capacity monitoring.
- High capacity air conditioner in the server and storage media rooms to prevent damage from heat and humidity.
- Locating the data center away from hazardous or high crime areas.
- Preventive maintenance monitoring.
- Preventive maintenance schedule.
- Redundant communication lines, servers and storage media, e.g., redundant array of independent disks (RAID). RAID is a technology used to write the same data to multiple disk drives. It is not a substitute for backup because the drives are controlled by the same server. Malfunction of the server can cause erasure of written data. RAID

mainly provides short term redundancy whereas backup provides long term redundancy. Servers should be configured to use RAID. For online systems that process a high transaction volume like banking and point-of-sales systems, redundant servers and communication lines are used. In many cases, the redundant servers and communication lines are actually used to record multiple copies of each transaction, for contingency. More organizations are moving towards virtualization, i.e., using software to pull servers together to tap unused hardware resources. Generally, this means putting more eggs in a basket. This increases the importance of redundancy planning and provision.

- Strong locks with multi-level barriers.
- Uninterrupted power supply including diesel battery and generator.
- Using fire retardant material for data center construction.
- Using raised floor construction to avoid floods.

For incidents that are beyond the control of organizations to prevent, reliance will be mainly on recovery controls. Such recovery controls will also be useful to recover from incidents that could have been prevented but were not prevented because of flawed preventive measures or because they were too expensive to prevent.

INCIDENT RESPONSE AND DISASTER RECOVERY CONTROLS

To ensure that operation is not significantly interrupted in the event of computer incidents and disasters, organizations should have internal controls in the form of policies, procedures, response teams, hardware, software and information. These controls should be formulated with coordination of the user areas and periodically validated. Recovery controls are really of a corrective nature. One might wonder why we have skipped detective controls. Controls to detect incidents that affect system performance will be discussed below under Network Monitoring Controls. Disasters do not need controls to be detected because their occurrence and impact are usually felt immediately.

Data Retention and Backup

A common risk in information systems is the loss of data. A rigorous backup schedule should be followed. The backup files must be kept offsite to avoid total data loss when the site that holds the original files is unreachable. Organizations should use automated backup tools such as electronic vaulting or storage access networks to ensure regular backup and avoid physical transfer of disks and tape. Backup logs should be reviewed periodically and backed up data should be retrieved for testing to ensure it is comprehensible. Employees should be given network folders to store their work files and be reminded not to store work files on local hard disks. Electronic vaulting uses online transfer of data to backup servers without using computer tape. A storage access network provides cross-departments and cross-locations storage of backup with online access; i.e., it is a LAN or WAN used only for backup. There is a trend in using cloud for backup. This is cheaper but security is a concern. We will discuss this more in Chapters Five and

Eight. When adopting cloud backup, an organization should be diligent in researching the reliability of the vendor or service provider (especially when it is free), and the service contract should cover availability and security assurance.

Software Backup

Source, object and executable code should be backed up as it is changed. Because organizations tend to implement system changes only at night so as not to contend for system time with transaction processing, backing up software daily is enough. Smaller organizations may adopt even a weekly or monthly backup schedule, or when it is known that source code or object code has been changed.

Data Backup for Batch Systems

A batch system is one that updates data files at fixed intervals instead of when every transaction occurs. Examples of transactions that are processed on a batch basis are bill payments by customers, payroll and deposited checks. Even if we pay bills online and the money is deducted from our bank accounts right away, the payee does not get the money from our bank until the end of the day and therefore our account with the payee company will only be updated at the end of the day or the next day. Data backup for a batch system should be performed daily.

In every transaction system, there are two types of data files, master file and transaction file. A transaction file typically contains every transaction processed within a period. A daily transaction file consists of the transactions processed that day. Tomorrow, a new transaction file will be started.

A master file contains permanent and semi-permanent information. An example is a credit card account file. This file contains the cardholder name, card number, balance, interest rate, address, credit rating and recent transactions. This file is updated periodically by transactions.

Backed up transaction files should be kept long enough to satisfy Canada Revenue Agency or Internal Revenue Service requirements as appropriate. That usually means seven years. To save space, the backup software usually compresses the backed up files. The backed up file should not be confused with the archived original files which are also compressed. The backed up file is an extra copy and should be kept off site.

The backed up master files do not have to be kept as long. A master file is not a file of history; instead it evolves. Yesterday's master file has been superseded by today's. Therefore, the importance of old master files is less than that of old transaction files. If an old master file is lost, it can be recreated using the transaction files and the master file previous to the one that has been lost. An organization should keep the original master file versions long enough to satisfy financial statement audit requirements. How long

should the backup copy of old master files be kept? Industry standard indicates that the minimum should be three versions, i.e., the backup of the last three master files should be kept. This is often called the grandparent-parent-child approach. This approach involves a shorter cycle than that normally used to keep the original master files because the backup files are needed only if the original files are lost or damaged. In practice, most organizations surpass the grandparent-parent-child standard for backup retention. Grandparent-parent-child is more a concept than a limit in terms of the number of generations of backup master files to be kept.

How long should the original master files be kept? Even though a master file can be recreated from transactions, such recreation can be time consuming and prone to errors. The time it takes to recreate a master file may make the recreated file too late to satisfy business requirements. It is therefore important to keep the master file versions for a safely long period. The general convention is to keep them for two years, to allow enough time for financial reporting for the fiscal year to complete. After two years, old master files are seldom needed.

Data Backup for Online Systems

The requirement for transaction file backup is the same as that for batch systems because after a transaction is processed, the criticality of transaction data is the same between a batch system and an online system. As indicated earlier, because of the high frequency of online transactions and the higher likelihood that they are paperless, large companies can use redundant servers and disks to write every transaction to multiple devices and this satisfies the back-up requirement, because the multiple recording will also update multiple copies of the master file. If this redundancy method is not used, the master file should be backed up more frequently than once a day because the master file is updated when every transaction occurs. The master files change throughout the day, so backing it up only at the end of the day presents a major risk. For example, if the master file is damaged at noon, the organization will operate with significantly non-current master file information. Although the master file can be recreated from yesterday's master file and today's transaction file, that will take time and until it is completed, the organization will be operating with non-current balances. It is therefore critical to back up the master file several times a day. The end of day master file and transaction file should also be backed up.

Data backup should not be confused with data retention. Data should be retained sufficiently long to meet operational, financial reporting and statutory requirements. Backup is done to mitigate the risk of business interruption caused by the loss, damage or destruction of the original data files. Organizations should have a retention schedule.

Incident Response Procedures

Although computers are fast and inherently accurate, its interface with people is not without glitches. Human to human interface is easier to comprehend and problems can be detected more interactively than computer to human interface. In the last chapter, we talked about the risks of computers going down, computer programs being wrong and people misusing information systems etc. These incidents can lead to unreliable information and financial loss. Organizations must have a set of procedures to address incidents.

A large number of incidents are security related. This is why the incident response procedures in many organizations are developed and maintained by the security department. However, the impact on the organization and the urgency for action are often the same between security incidents and non-security incidents. The escalation and remedial action depend on the incident's severity.

Incident response procedures should guide management in determining an incident's severity. For example, it is common in governments to rate an incident as severity level 1, 2, 3 etc. The severity level would call for different amount of resources and different layers of management to be involved in investigation and resolution.

Incident handling usually starts with the IT help desk. In cases where the incident cannot be resolved, procedures should be followed to escalate it to level 2 support. Level 2 support is staffed by subject matter experts. If the incident cannot be resolved there, it should be escalated to level 3 and so on. It is rare for an organization to have more than five levels in terms of technical support because the more levels there are the more bureaucratic the process will become. Meanwhile, the procedures should guide staff to keep management informed on an escalating scale.

<u>Sample Information Systems Incident Response Procedures</u>

1) An incident may be discovered by any of the following areas.
    a) Help desk
    b) Intrusion detection monitoring personnel
    c) A system administrator
    d) A firewall administrator
    e) A business partner
    f) A manager
    g) Information Protection Centre (IPC)
    h) An employee
    i) A customer
    j) Another outside party

2) If the initial discovery is made by someone other than a security administrator, the help desk or the IPC, it should be reported to the following units in the order of availability.
   A. IPC at 4164972882 and ipc@wiletec.com.
   B. Help desk at 9059409515 and ithelp@wiletec.com.

   Reporting should be done by email and telephone, with email following the phone call. If the IPC does not answer, leave a voice mail and call the help desk. In either case, an email must be sent to the IPC following each incident reported by phone. If an incident is discovered by a security administrator or the help desk, it must be reported to the IPC by phone and email.

3) The help desk and IPC should log the following.

   a) The name of the caller.
   b) Time of the call.
   c) Contact information about the caller.
   d) The nature of the incident.
   e) What equipment or persons were involved?
   f) Location of equipment or persons involved.
   g) How the incident was detected.
   h) When the event was first noticed that supported the idea that the incident occurred.

4) The IPC will gather the following information:

   a) Is the equipment affected business critical?
   b) What is the severity of the potential impact?
   c) Name of system being targeted, along with operating system, Internet Protocol (IP) address, and location.
   d) IP address and any information about the origin of the attack.

   The IPC will contact the business division incident response manager.

5) The IPC and the business division incident response manager will meet (eConference is fine) to discuss the situation and determine a response strategy. The following questions will have to be answered.

   a) Is the incident real or perceived?
   b) Is the incident still in progress?
   c) What data or property is threatened and how critical is it?
   d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
   e) What system or systems are targeted, where are they located physically and on the network?
   f) Is the incident inside a trusted network?
   g) Is the response urgent?

h) Can the incident be quickly contained?
i) Will the response alert the attacker?
j) What type of incident is this? Exampled are virus, worm, intrusion, abuse and damage. An incident ticket will be created.

The incident will be categorized as follows:
Category one - A threat to safety or life.
Category two - A threat to sensitive data
Category three - A major threat to computer system reliability
Category four - A minor threat to computer system reliability

6) Team members will follow one of the following procedures as needed to formulate their response on the incident assessment:

a) Worm response procedure
b) Virus response procedure
c) System failure procedure
d) Intrusion response procedure - is critical data at risk?
e) System abuse procedure
f) Property theft response procedure
g) Website denial of service response procedure
h) Database or file denial of service response procedure

7) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection and prevention logs, and interviewing witnesses and the incident victims to determine how the incident was caused.

8) If hacking has been determined to be successful or there is internal compromise, the IPC will contact the Forensic Team.

9) The Forensic Team will seek advice from the Forensic Manager and if a formal investigation is deemed necessary, seek the approval of the Vice-president of Information Security to start an investigation.

10) Team members will recommend changes to prevent recurrence.

11) Upon management approval, the changes will be implemented.

12) Team members will work with IT operations to restore the affected system. They may do any or more of the following:

a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
b) Make users change passwords.
c) Be sure the system has been hardened by turning off or uninstalling unused services.

d) Be sure the system is fully patched.
e) Be sure real time virus protection and intrusion detection are running.
f) Be sure the system is logging events.

13) Documentation - the following shall be documented:

a) How the incident was discovered.
b) The category of the incident.
c) How the incident occurred, whether through email, firewall, etc.
d) Where the attack came from, such as IP addresses and other related information about the attacker.
e) What the response plan was.
f) What was done in response?
g) Whether the response was effective.

14) Evidence preservation—make copies of logs, email and other communication. Keep lists of witnesses. Keep evidence for seven years after resolution.

15) Notify proper external agencies - notify the police if there is criminal implication and inform the legal department.

16) Assess damage and cost - assess the damage to the organization and estimate both the damage and the cost of the containment efforts.

17) Review response and update policies - plan and take preventive steps:

a) Consider whether a new procedure could have prevented the intrusion.
b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
c) Was the incident response appropriate? How could it be improved?
d) Was every appropriate party informed in a timely manner?
e) Were the incident response procedures detailed and did they cover the entire situation? How can they be improved?
f) Have changes been made to prevent recurrence? Have all systems been patched, locked down, passwords changed, and anti-virus updated?
g) What lessons have been learned from this experience?

Disaster Recovery Plan

Every organization that relies on information systems should have a disaster recovery plan to help it recover from accidents and disasters. This plan should be more extensive than incident response procedures. To prepare the plan, an organization needs to first understand its information systems risks and business critical systems. A business impact analysis (BIA) should be performed for each business critical system. The list of business

critical systems discussed in the first chapter would be a strong basis for determining the complexity of the plan and the priority of recovery. Companies in certain regulated industries are required to maintain a current disaster recovery plan.

The disaster recovery plan should consist of the following:

- Types of disasters.
- Criteria for calling an incident a disaster and ranking disasters.
- Authority for calling disasters.
- The disaster recovery team, i.e., the people who will be called on to manage disasters. Key contact information should be kept current.
- Automated tool to contact the team, e.g., an organization can use an automated tool that has stored multiple contact points for each team member and at one click, the tool will send online notification to the team members within seconds.
- Disaster recovery procedures to include:
    - damage control
    - moving people and equipment
    - locating backup data and equipment
    - protecting systems that are still operating
    - resuming broken systems.
- Provision for alternative processing facilities, which may be a hot, warm or cold site.
- Priority of systems for recovery.
- Process and responsibilities for communication to executives, stakeholders and customers.
- Procedures for recovering from the disaster.
- Common scenarios and case studies on how they are responded to.
- Schedule of testing.
- Test criteria.

Some organizations call this a contingency plan. A contingency plan is actually wider in scope. It addresses more than just IT resources, e.g., space for office workers, how to deal with the press. In this book, we will study disaster recovery planning instead of contingency planning.

The disaster recovery plan (DRP) should be tested annually and a copy must be kept at an alternate location that is reachable to the team. The disaster recovery plan needs to be supported by regular data backup procedures, as without backup, it would be difficult to recover from a disaster.

The DRP should be developed based on a comprehensive BIA. BIAs should be performed by business unit executives who will charge their teams with preparing the assessment. The IT department can provide technical assistance in terms of the effect of IT disasters on business units. The process for system ownership and risk assessment discussed in Chapter Two should be applied to BIA. The business unit BIAs should be rolled up by the chief risk officer, and in the absence of that function, by the CIO. The

business unit executives, chief risk officer and CIO will work together to prioritize the list of systems to be recovered in situations of limited resources. This list should be approved by the IT steering committee and in the absence of that committee, by the CEO.

The DRP is then developed by the IT department to ensure that there are significant IT resources to resume operation of the business critical systems within the tolerable periods of system outage. These systems are generally classified as tier 1, tier 2 and tier 3 etc. For example, a tier 3 system may be a system whose outage is tolerable up to a week. Subsidiary to the corporate DRP, there is a separate DRP for each business critical system. The system specific DRPs should be approved by the system owners.

The DRP should be tested at least annually. Often, regular testing may take several rounds, e.g., when testing reveals a deficiency in the DRP or associated procedures, the deficiency must be fixed and testing will be reperformed. A test that reveals deficiency in the disaster recovery plan is a successful test. Tests should be reviewed by the people who developed the DRP and DR team representatives. Test results should be signed off by the CIO.

Alternative Data Center

A DRP has to be supported by an alternative data center. Such an alternative data center can be a hot site, a warm site or a cold site. It may be sourced internally or contracted. The type of site and the extent of equipment in each site depend on risk assessment, i.e., the business criticality of systems and the risk that the organization wants to take. The organization's budget also affects the type of sites.

A hot site is one that is immediately available. It has hardware and software available, although not necessarily with the same capacity as the primary data center. A warm site usually has more limited hardware and software, so in the event of a disaster, it may take a couple of days to activate. A cold site has the premises but no hardware and software; the organization will have to make arrangement or call vendors to honor an existing agreement to install hardware and software in order to make the site functional. For each type of site, the site provider may be a company that specializes in disaster recovery facilities or a trading partner. The site may also be an internal facility. The backup site should be reasonably apart from the primary site to make the former easily reachable while minimizing the risk of both sites being destroyed by an accident. A rule of thumb is forty miles. An organization may use a combination of hot, warm and cold sites. For example, it may operate a hot site for its tier 1 systems and a warm site for its tier 2 systems.

TECHNOLOGY INFRASTRUCTURES CONTROLS

These are controls to ensure that information systems are operated as scheduled and as needed. They include the following.

- Procedures to guide IT purchases
- Processing schedule
- IT deployment procedures
- Technology infrastructures procedures
- Network documentation
- Server and network configuration
- Network transmission controls
- Service level agreements

Controls over IT Purchases

Every organization should have purchasing policies and procedures to ensure approval and value for money. These policies and procedures should apply to IT procurement. The risk presented by IT purchases goes beyond cost. Management should be aware of the total cost of ownership (TCO) of hardware and software, even if software is leased or paid for as annual licenses. TCO includes the purchase, lease or license cost, the maintenance charges by vendors, maintenance cost incurred internally, the cost of training and the disposition cost. Therefore, the approval levels for initial purchase, lease or license should be determined by considering TCO. For example, if TCO is $100,000, approval should be obtained from a manager with signing authority of $100,000.
Aside from cost, organizations should control the acquisition of software to ensure that the software is compatible with the organization's IT platform. A company using Windows throughout will not want people to go to a store to buy computers using other operating systems to connect to the company network without approval.

The acquisition policy and procedures should define who can request hardware and software, who will do the actual procurement and who will approve. The criteria for approval and justification should be stated. There should be periodic verification of inventory.

It is increasingly common for large organizations to set up a portal for employees to request hardware and software and for such requests to be routed to management for approval. The approved requests will then be sent by the portal to the procurement department; i.e., employees are not allowed to go to a retail store or an online vendor to buy hardware or software. An organization should negotiate bulk discounts with hardware and software vendors.

Controls over IT purchases support the control criteria of accuracy, authorization, occurrence and efficiency.

Processing Schedule

There should be management approved schedules to control network and system availability as well as when batch processing is to be carried out. The schedules should be monitored using software and deviations should be reported for explanations. The schedule should also be periodically reviewed to ensure that it meets business requirements and use hardware resources optimally. Process scheduling controls support the criteria of completeness, accuracy, timeliness and efficiency.

Hardware and Software Deployment Procedures

In addition to controls over IT purchases, organizations should have established procedures to make sure staff are aware that installation of hardware and software must be approved by management and performed by designated specialists. This prevents inappropriate use of hardware and software which can violate maintenance agreements or licenses and cause system instability. These procedures will also help ensure that the organization knows exactly what computers are connected to the network, which is important for network monitoring. There should be monitoring controls to alert management of installed hardware or devices such as installing a wireless access point, for network managers to ensure that such installation was approved and was done in accordance with established procedures.

The organization should have standard configuration parameters for hardware and software to ensure consistency throughout the organization. There are network tools that allow organizations to audit such configuration from server to server and from desktop to desktop. Staff should be prevented by the network from changing the configuration of their desktops or laptops. For example, a bank employee's office network ID gives that person ordinary user access to his or her computer, instead of "administrator" access, so s/he cannot install software.
Hardware and software deployment procedures support the control criteria of completeness, accuracy, authorization and efficiency.

Network and Hardware Operation Procedures

There should be procedures to guide system and network administrators to perform routine maintenance and respond to user questions. These procedures should be consistent with the processing schedule described earlier and the configuration procedures. Network and hardware operation procedures should be stored away from the servers to which the procedures apply to prevent losing a server and the procedures for running that server simultaneously. Network and hardware operation controls support the criteria of completeness, accuracy, authorization and efficiency.

In Chapter One, we mention the roles of the system administrator and database administrator. The former has full control of the assigned server and can change data and programs. The latter has full control over the database. These two functions must be separated because either one is powerful enough to cause significant damage if the employee is careless, not well trained, or rogue. Also, the operating system should be configured to log all database activities carried out by the database administrator (DBA) and the DBMS should be configured to produce management reports on the DBA activities for regular review. Operating systems should have the default setting of logging all system administrator activities and IT management should install software to take the operating system log and produce management reports for regular review.

Network Documentation

Network documentation is critical for an organization to plan and implement network changes, move servers and troubleshoot. Such documentation should include a minimum of network topology diagrams and related narrative description. It should be developed when the network is built and updated as necessary, especially after a network relocation or major system implementation. The documentation should be periodically verified to ensure currency. It should be protected from unauthorized access especially access through the Internet. Network documentation supports the criteria of completeness and accuracy.

Server and Network Configuration

Organizations should have a policy and set of procedures to guide such configuration, including a standard checklist compiled based on risk assessment. Configuration should be periodically reviewed to ensure it reflects the current policy, standards and procedures. The standard configuration should be saved as a software image for deployment on multiple servers and workstations to ensure consistency. Server and network configuration controls support the criteria of completeness, accuracy, authorization and efficiency.

Network Transmission Controls

It is preferable to prevent errors rather than to rely on error detection and correction. Preventing transmission errors involves choosing physical media with low inherent data error rates and taking suitable care in designing physical and logical circuit configurations. For example, wires should be properly shielded, voice and data lines should be reasonably apart to avoid cross-interruption (cross talk). The choice of circuit also affects the error rate. Fiber is less susceptible to environmental interruption than telephone line and copper. Network transmission controls support the criteria of completeness and accuracy.

Networks should be monitored continuously to ensure availability, stability and efficiency. Organizations should have redundant servers and dynamic load balancers to minimize outage and bottleneck. Network tools should be run to identify bottlenecks. Network reports should be reviewed by management and an audit trail of corrective actions should be maintained. Data transmission redundancy should be built in to avoid data loss. A variety of methods of transmission redundancy should be deployed depending on the reliability of the communication circuit, the sensitivity of data and the cost of error correction. The common methods are parity check, redundant data check and echo check.

The ability to detect errors depends on the inclusion of extra data at the sender's end that can be verified at the receiver's end. The extra data is used only for error detection and will be discarded after the detection process. This extra data is called error detection value. You should understand the trade-off between using more or less error-detection value. Including more data increases the ability to detect errors, but also slows data transmission because of the extra data needed to be sent with the message. This is analogous to airport security.

Computer data is in bits and bytes. There are usually 8 bits in a byte. A byte can represent a character or a number. A byte usually can accommodate a maximum number of 256. Therefore a large number usually takes several bytes. Bytes are combined into a packet. An organization will adopt a packet size that is optimal for data transmission. The purpose of packetization is to allow a transaction or message to be broken into smaller strings of bytes (packets) so that the packets can travel in different routes to avoid bottle neck, i.e., finding the fastest combination of routes to the destination. It is similar to dividing an army into groups so they can find small openings to get through to the destination and once at the destination, they will be regrouped. We will discuss this more in Chapter Five.

Parity Check

This simple and old form of data transmission check method can detect about 50% of errors. This does not mean that data transmission using this method of detection is only reliable half of the time, because errors, in the first place, may seldom occur depending on the quality of circuit. Parity checking involves using the last bit of every byte as the check bit. A network can adopt the even parity mode or the odd parity mode. In even parity, the number of "1" bits in a byte, including the check bit, must be even; in odd parity, the number of "1" bits in a byte, including the check bit, must be odd.

If the network adopts the even parity mode, it will inspect every byte before transmission. If the number of "1" bits is even, the network will assign an additional bit as the check bit and make that bit 0. If the number of "1" bits is odd, the check bit will be assigned the value of 1. By so doing, the number of "1" bits in every byte, including the check bit, will be even. The receiving node (network point) can then count the number of "1" bits in

each byte to make sure it is even. If it is odd, that means one or more bits have been changed along the way by a system software glitch, hardware malfunction, environmental condition or hacker.

For example, an organization that adopts parity check will use only the first 7 bits of a byte to represent data and use the 8^{th} bit for parity check. When the even parity mode is used and before setting the parity bit, if the 7 data bits are 0101011, the parity bit will then be set to 0, so that the number of "1" in the full byte will be even; if the first 7 bits are 0101001, the parity bit will be assigned the value of 1.

The receiving node must be programmed to discard the check bit after checking for transmission accuracy. The receiving node may be in another organization, in which case, the sending organization will have to make that kind of agreement with the receiving organization, i.e., adopting even parity or odd parity.

If an even number of bits in a byte are off (either from 0 to 1 or vice versa), parity checking will not detect it, because of offsetting errors.

Redundant Data Check

This method is applied to a message, transaction or packet, instead of individual bytes. A packet contains a number of bytes. A standard packet contains 1,024 bytes. In applying this method, the message or packet to be transmitted is treated as a long binary number. A fixed number is then divided into the message to obtain a remainder. Common lengths of the divisor are 8, 16, 24 and 32 bits, with the most significant bit being 1. The longer the divisor, the more reliable the method is, up to the point where the divisor reaches half of the value of the dividend.

The remainder is added to the message as the error detection value. The receiving node will repeat the calculation and compare the calculated error detection value with the received error detection value. A divisor of 16 bits with the most significant bit being 1 can detect almost 100% of errors.

Echo Check

This means the receiving node returns what it receives for the sending node to check that it equals what was sent. This is usually done at a packet level. This is expensive as it doubles the traffic. However, it is very reliable as any missed bits will most likely be detected. We say "most likely" because there is still a risk of offsetting errors. For example, a bit accidentally becomes "off" in transmission; the receiving node returns a copy of the received packet to the sending node for comparison with a copy of the sent packet kept by the sending node. However, when the "wrong" packet copy is returned to the sending node for confirmation, the same bit is accidentally set to the "on" value (1) in transmission, now the sending node of course will confirm that the received value is the

same as the sent value when in fact it is not. A node is a network connection point like a router, switch or server. Echo check is more reliable than parity check and redundant data check that uses a divisor that has fewer than sixteen bits.

Error Correction

If an error is detected by the receiver, it is usually corrected by retransmitting all or part of the message. However, when the distance is great such as in satellite transmission, retransmission can be too costly and the retransmitted data may be too late and affects usefulness, e.g., critical video or financial data. In such a case, the network should send enough data to facilitate error correction to take place automatically. This is called forward error correction. The extra data to be sent for error correction usually amounts to 50% to 100% of the original data. The use of the forward correction method should be based on comparison of the cost of extra data transmission and the delay involved in retransmission.

Service Level Agreement

The IT department of an organization often receives more requests for services than its resources can accommodate. It is important for the CIO to adopt a consistent methodology to review and prioritize user requests and communicate the response to such requests clearly and on a timely basis. Part of the methodology should be a costing mechanism that will be used to charge users for the cost of providing the services. When a user department is charged with cost, it will think carefully before requesting service. Once a service is promised for delivery, the users should know when to expect delivery, the basic quality expected and how to escalate problems. The above information, e.g., deliverables, cost, deadlines and problem escalation channels, should be documented in a service level agreement between the IT department and each major user department. These agreements will be similar but tailored to the business needs of individual user departments. However, the IT department should not charge market rates because it is not supposed to make a profit. A service level agreement supports the control criteria of completeness, accuracy, authorization, timeliness and efficiency.

Capacity Planning

Organizations should continuously monitor their infrastructure to assess stability and adequacy to support the IT strategy. Current technologies like cloud computing and virtualization should be considered to increase scalability. The capacity plan should be updated at least annually and should cover, hardware, network and the alternate data center.

Cloud computing offers the following benefits:

- On demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity

An organization can choose to have a private cloud, community cloud, public cloud or a combination of the above three. A community cloud is provided for use by a specific group of network users or network user organizations. These three types vary in security, availability and cost proportionally.

INTELLECTUAL PROPERTY CONTROLS

Information technology enables organizations to be more innovative. As a result, there is increasing reliance on intellectual property purchased or developed. Intellectual property purchased such as software should be protected from unauthorized use and this can be done mainly with access controls.

Intellectual property developed warrants more attention. It must be protected from unauthorized use and infringement of the property ownership. Access controls are critical. Also important are license contracts, contract compliance audits, non-disclosure agreements with employees and contractors, as well as registration with the appropriate intellectual property government offices under legislations such as the Copyright Act.

We will discuss intellectual property in more detail in Chapter Five.

MANAGEMENT CHECKLIST

1. Develop an IT strategy to be congruent with the business strategy.

2. Develop an IT directive or policy to provide high level guidance and a structure for IT practices including IT controls.

3. Develop and keep up to date IT organization charts that support segregation of duties between the IT functions and user areas as well as among the IT functions.
4. Develop and update job descriptions to provide clear direction of responsibilities and to support segregation of duties.

5. Develop IT policies and procedures to implement segregation of duties, security, software change controls, technology infrastructures controls, privacy protection, disaster recovery controls and network monitoring.

6. Maintain separate libraries and environments for systems development, integration testing, user acceptance testing and production.

7. Establish an IT steering committee to oversee IT expenditures and review major projects.

8. Develop and regularly test a disaster recovery plan.

9. Implement procedures to monitor network reliability and efficiency.

10. Ensure that IT controls are thoroughly documented and assessed annually for effectiveness.

CONCLUSION

Today's business environment is a lot different from what it was when computers were first used to process transactions. Most business systems in large organizations are now open to the public directly or indirectly. There are more system users and they expect more in terms of system efficiency and reliability. Today's customers are less loyal and patient. Just look at the telephone and TV markets. Consumers can switch phone company, TV carrier and Internet service provider with a few clicks. Regulators are more demanding on companies to implement sound internal controls.

Internal controls are no longer just the interest of auditors. Managers are increasingly convinced and comfortable about their control ownership and responsibilities. They need help, help from industry guidelines, internal control specialists, control systems and auditors. An increasing percentage of business functions are automated. Management and auditors have to continuously keep up with the control implications of technology and using technology to achieve business competitiveness and reliability. Competitiveness and reliability can no longer be separated, and internal controls provide the bridge.

SUMMARY OF MAIN POINTS

Although most internal controls operate daily and are at the transaction and data levels, the extent of controls and their responsibilities stem from the control environment and culture that senior management has created and shaped over time. Senior management does that by exercising IT governance.

In this chapter, we have focused on those IT controls that are pervasive in the organization across business areas, and they are called general controls. There are IT controls that are specific to individual business systems. Those are called application controls and we will discuss them in Chapter Six.

Internal controls can be preventive, detective or corrective. Preventive controls are preferable to detective controls. However, an organization needs both because it is impractical to prevent all major errors and irregularities. For each detective control, there should be a corresponding corrective control.

General Controls

- Organization controls – including segregation of duties between IT and users as well as within the IT department.
- Access controls – we will discuss them in detail in Chapters Eight and Nine.
- Software change controls.
- Systems development controls – to be discussed in the next chapter.
- Disaster prevention controls.
- Disaster recovery controls.
- Technology infrastructure controls.
- IT performance measurement controls.
- Intellectual property controls.

Organization Controls

- I&IT strategy.
- IT steering committee.
- Policies and standards.
- Segregation of duties.
- Documented consistent hiring practices.
- Code of business conduct.
- Training.

Access Controls

- Physical
- Logical (data and software).
- Applies to infrastructure, software, people, information and procedures.

Software Change Control

- Application software change control.
- System software (e.g., operating system) change control.
- Change control policies and procedures.
- Naming conventions.
- Library control.
- Separate environments for development, testing and production (operation).
- Software testing.
- Change approval.

- Change monitoring.
- Procedures to deal with emergency changes to ensure adequate testing, documentation and approval.
- Code comparison.

Systems Development Controls
- Systems development methodology
- Approval at checkpoints
- Documentation standards

Disaster Prevention Controls
- Hardware and network redundancy
- System backup and offsite storage
- Data backup and offsite storage
- Backup testing
- Fire and water resistant data centers
- Locating data centers away from hazardous or high crime area
- Preventive maintenance schedule and monitoring
- Hardware performance monitoring

Disaster Recovery Controls
- Incident response procedures
- Disaster recovery plan
- Disaster recovery testing
- Disaster recovery site (alternative data center)
- Secure disaster recovery site away from the primary data center

Technology infrastructure Controls
- Service level agreement
- Operations procedures
- Procedures for hardware purchases and deployment
- Hardware configuration standards and procedures
- Network transmission control
- Operation schedule

REVIEW QUESTIONS

1. What is the relationship between software change controls and systems development controls?

2. Who should approve the corporate disaster recovery plan?

3. How often should a disaster recovery plan be tested?

4. Who should the CIO report to?
5. What is the best approach to moving software to the production library?
6. What is the difference between an environment and a library?
7. What does an auditor see in an organization chart?
8. What is the drawback of parity check?
9. How often should a bank back up its transaction files and why?
10. What kind of system is the grandparent-parent-child backup approach used for?

RUNNING CASE – Blackberry

Develop a disaster recovery plan.

MULTIPLE CHOICE QUESTIONS

1. How does the Investor Confidence Rules affect IT governance? It
   A. requires management to certify internal controls.
   B. prohibits an accounting firm from providing consulting service to an audit client.
   C. requires the appointment of a chief risk officer.
   D. requires the appointment of a chief privacy officer.
   E. requires the rotation of auditors every five years.

2. In which environment is source code accessed the most?
   A. Production
   B. Development
   C. Testing
   D. Staging
   E. Audit

3. Which of the following is an internal control?
   A. Segregation of duties.
   B. The organization will hire only honest employees.
   C. Software change requests must be approved by the manager of change control.
   D. Source code must be compiled to object code before user acceptance testing.
   E. Information system risks are assessed annually.

4. Which environment should a program be sent to if user acceptance testing reveals an error?
   A. Development
   B. Testing
   C. Production
   D. Programmer
   E. Backup

5. Which is the most effective control over system administrators?
   A. Code of ethics
   B. Reference check
   C. Supervision
   D. Management review of activity log
   E. Performance appraisal

6. Who are responsible for IT governance?
   A. Chief financial officer
   B. Chief risk officer
   C. Chief auditor
   D. Senior executives
   E. Board of directors

7. Which of the following is a back-up procedure?
   A. Keeping transactions for seven years
   B. Compressing historical transactions
   C. Sending historical transactions offsite
   D. Keeping a duplicate of the master file
   E. Keeping the computer printouts and the master file

8. Which one is a correct one-to-one correspondence?
   A. Library and environment
   B. Programmers and testers
   C. Source code and executable code
   D. Master file and transaction file

9. Which of the following libraries can be accessed by programmers extensively?
   A. Test
   B. Development
   C. Staging
   D. Production

10. Which of the following statements represents an undesirable practice?
    A. Appointing the chief auditor to the firm's IT steering committee
    B. Assigning accountants to systems project teams
    C. Hiring consultants to work on systems development projects
    D. Asking the chief information officer to participate in business strategic planning

CHAPTER FOUR – SYSTMS DEVELOPMENT CONTROLS

You must be the change you want to see in the world. - Mahatma Gandhi

The average organization spends about half of its information technology (IT) budget in developing systems. Systems development is not trivial and most organizations do not do as well as they would like to. Many systems development projects are not completed on time and on budget and do not meet all user requirements. Organizations need to have a discipline in developing systems. Systems are developed more frequently these days as the life of a system is shorter. The life is shortened in a way by international competition which compels organizations to change to keep up with the industry. eBusiness has empowered small organizations to compete with multinationals. Small companies can change their systems more dynamically as they have less overhead and fewer organizational layers to go through; they are also more adventurous.

Twenty years ago, the average systems development project took 3 to 5 years to complete. Today, if implementation does not start 2 years from project initiation, the organization may be falling behind its competitors or customer expectation. It is important to maintain discipline and practice controls while speeding to meet business challenges in systems development.

EXAMPLES OF SYSTEMS DEVELOPMENT PROJECT SHOFTFALLS

Here is a list of systems development projects that did not succeed as expected or had significant bugs after implementation.

1. A Toronto company hired a large consulting firm to develop a leading edge system to increase market share. After a few months on the job, the new CEO terminated the project and wrote off millions of capitalized project cost. This was the chief operating officer's pet project. Managers approved invoices from the consulting firm without ensuring that the deliverables were acceptable. Users complained about the project progress and the usefulness of functions that had been delivered.

2. In June 2012, social workers in British Columbia, Canada said a new computer system that handled thousands of files for the Ministry of Social Development and the Ministry of Children and Family Development was plagued with problems and wasting valuable time. The $180-million Integrated Case Management System was designed to enable social ministries to share information, but an internal document obtained by the New Democratic Party says the system was prone to breakdowns and is almost impossible to use. Employees said they sometimes had to take hours to enter data or search clients' history, and information could get lost in the process. The new system was designed to replace 64 different databases.

3. In 2008, the Heathrow Airport Terminal 5 new baggage handling system produced wrong flight status information to the baggage crew. This resulted in bags not getting loaded to the right planes. One estimate was that this crisis cost the airlines £50m.

COMMON REASONS FOR SYSTEMS DEVELOPMENT PROJECT FAILURES

Here is a list of common pitfalls in managing systems development projects.

- The project is too big and therefore difficult to manage – A solution is to break it to more manageable projects that can be carried out concurrently with different project managers or successively if resources are limited.
- No senior management accountability thus leading to insufficient monitoring – An executive sponsor should be assigned to each project, who should also be the system owner.
- Insufficient project reporting to senior management – There should be a process for periodic reporting to the project sponsor and the IT steering committee.
- No post-implementation validation of project success – There should be an independent post-implementation review.
- Lack of project management skill thus leading to poorly coordinated projects – Large organizations should establish project management offices as centers of excellence in project management.
- Insufficient project planning thus leading to a project running off the wrong direction – An organization should have a standard for project planning. If you fail to plan, you plan to fail.
- Insufficient management and user signoffs thus leading to wrong deliverables or missed deliverables – An organization should require signoffs at multiple stages of a project.
- Insufficient business case thus leading to a system that is not cost effective – A business case should be required before the project sponsor signs off the project plan.
- Inadequate system design thus leading to a system that does not meet business requirements – An organization should have a standard and rigorous procedures for systems design.
- Inadequate requests for proposals for purchased systems thus leading to buying the wrong systems – An organization should charge the project sponsor with assigning business users to write the request for proposals (RFP) and for the RFPs to be approved by project sponsors.
- Changing user requirements thus leading to projects that are late or don't get finished – An organization's systems development methodology should not allow user requirements to be changed after signoff unless the project sponsor approves.
- Resistance to change thus leading to project delay – The systems development methodology should include a communication plan for the project to ensure the affected staff receives proper and timely information about how they will be affected.
- Inadequate testing thus leading to unreliable systems – The systems development methodology should require different stages of testing and signoffs.

- Inadequate training thus leading to ineffective use of a system – Training plans and signoffs evidencing receiving of training should be part of the systems development methodology.
- Lack of user involvement thus leading to systems that do not meet business requirements – An organization's systems development methodology should require detailed requirements to be signed off by the project sponsor. Frequent meeting with user representatives should be held to allow for status reporting and checkpoint reviews.
- No software change controls thus leading to effective programs – The software change controls discussed in the last chapter will help prevent this.
- Incorrect data conversion thus leading to systems with wrong opening data – An organization's systems development methodology should require user sign-off of data conversion.

ANNUAL SYSTEM DEVELOPMENT PLAN

Organizations have limited resources. Resources have to be allocated to desired projects based on the business cases and each project's congruence with the IT strategy. As part of the IT strategy, there should be an annual plan of systems development projects, i.e., what systems will be developed this year, next year, the year after, and year 4 etc. The annual plan should look forward at least three years and include current projects. The project management office (PMO) should be responsible for developing and monitoring this plan, i.e., monitoring the progress of systems development projects.

SYSTEMS DEVELOPMENT METHODOLOGY

Each organization should have a systems development methodology. The methodology should include the following.

- Definition of a systems development project versus a software change request. A systems development project is developing a new system or a major modification of an existing system, rather than an ad hoc or minor system change.
- Process for project initiation, business case preparation, project approval to proceed and project monitoring.
- Guidelines for system acquisition as well as managing vendors and consultants.
- Program naming convention.
- System documentation standard and format.
- Definition of each phase in systems development, the stakeholders and parties responsible:
  - Problem definition.
  - Feasibility study.
  - Project proposal including a business case.
  - System analysis.
  - Detail project plan.
  - User requirements.
  - System architecture.

- System design.
- Programming.
- System integration testing.
- User acceptance testing.
- Policies and procedures development.
- Update of the disaster recovery plan.
- Management approval to implement.
- Conversion.
- Implementation.
- Post-implementation review.
- Project monitoring and reporting, this occurs throughout the project.

The software change management controls that we talked about in the last chapter also apply to systems development projects because systems development requires software changes and implementation. In addition, a systems development project requires more controls related to project justification, project monitoring, documentation, testing, conversion, implementation, training and post-implementation review.

The key stakeholders that should sign off all or most of the above phases are the project sponsor, the project manager, the IT department, user area representatives, internal audit and the IT security function. The involvement and sign-off of internal audit are mainly to help ensure that adequate internals are built into the system and that the systems development methodology is followed.

PROBLEM DEFINITION

Before a systems development project commences, a business problem should be recognized and documented. The problem should be more than just an impulsive concern about operation. It should be a shortfall that has been sustained. A problem may also stem from a regulatory requirement, e.g., a reporting requirement from a regulator. A problem may be a requirement of a business strategy, e.g., to launch a new product. A problem may result from a directive or the law, e.g., a directive from the banking regulator or a new tax; in either case, a systems development project may have to be started to meet the directive or legal requirement. A system may be developed to seize a business opportunity, e.g., to expand market share. Whether the driver for a new system is a problem to address current shortcomings, to meet a legal or regulatory requirement, or to support new business direction, the need to justify the systems development project and manage it to successful implementation is the same.

A problem needs a champion unless it comes from the CEO or COO. The champion will solicit executive interest in the problem to a point where there is agreement that the problem has to be addressed potentially with a new system or a major system upgrade. The champion is likely someone who reports directly or indirectly to the executive with the biggest stake in the business area affected, i.e., the system owner. If there is no existing system to be replaced, the system owner would be the executive in charge of the

area that benefits most or has most control over the new system, e.g., the chief financial officer (CFO) for an accounting system, the vice-president of mortgage lending for a system to support a new mortgage product.

The next step is to conduct a feasibility study.

FEASIBILITY STUDY

The problem now has corporate recognition. The question to answer is whether it is solvable with a new system or a major system upgrade. Is a system solution feasible? There are three feasibility aspects to address: financial, technical and organizational. The feasibility study should be performed by the champion. The output is a feasibility report to be submitted to the system owner.

Financial Feasibility

This is actually a high level business case. At this point, the champion is not ready to ask for money. S/he wants to see if the system development project is financially affordable. This will involve understanding the financial atmosphere of the organization, e.g., is the organization facing significant financial pressure? It will also involve estimating the cost and benefit of the system without going into significant details. If the cost and benefit estimation indicates there is a convincing business case in light of the organization's financial health, financial feasibility can be demonstrated.

Technical Feasibility

The system required may be well ahead of the organization's IT infrastructure or skills. Although technology and skills can be purchased, a quantum leap increases the risk of project failure and management may hesitate to approve such a project unless it is required by law or to survive in the business. This is what technical feasibility is about.

Organizational Feasibility

The organization may be financially healthy, the system may have strong payback, the organization may have solid infrastructure and highly skilled developers, the idea to develop a system to solve the problem at hand may still be shot down if the organization has other significant problems or priorities to deal with. For example, if the new system will clash with the corporate culture, require significant re-organization, sends a message to customers, shareholders and taxpayers that the organization is taking a major risk in IT and business direction, or if the system introduces a major labor relations problem, the project request may not be approved. That's what organizational feasibility is about.

PROJECT PROPOSAL

If the feasibility study is approved, the project champion should initiate a project to find an IT solution for the identified problem. A proposal will be prepared and approved at ascending levels. The proposal should include a problem definition and a statement that is based on preliminary analysis, that a new system or a major system change is required. It should state at a high level, how the problem will be solved. Major projects may need to be approved by the IT steering committee or perhaps even the board before commencement. The level of approval depends on the cost of the project. Cost, for this purpose, means initial cost + annual net cost. Annual net cost = annual gross cost – cost reductions that have no strings attached, e.g., based on a signed contract that produces cost reductions. It is not net of benefits like projected increased profit or projected cost reductions generated by automation or efficiency. The latter items are subject to risks and may not materialize. This is why it is the initial cost + annual net cost (net of cost reductions with certainty) that should be used to decide how high up the proposal needs to be approved at.

The project proposal should also include a project risk statement to help the approvers assess the risks of undertaking the project. The risk statement should describe the types of risks and their probability. The suggested time frame for the project, as well as a breakdown of the types of resources by amount should be stated.

The proposal should include a business case that is based on the organization's business case methodology for capital projects, including the application of capital budgeting techniques. The business case should address the cost of hardware, software, vendor fees, consultants and salary.

Cost justification is primarily the responsibility of the project sponsor. This is usually the executive accountable for the function that the proposed system will support. For an accounting system, the sponsor is probably the chief financial officer. The sponsor usually does not have time for day-to-day management of systems development projects so s/he typically designates a project manager. The sponsor or a delegate should develop the cost-benefit analysis by engaging business and IT management. At this stage there is no assurance that the project will go ahead, and a project manager may not have been appointed yet.

Intangible benefits should be described in the business case. Intangible costs should be addressed in the risk statement. An intangible benefit may be better customer satisfaction, but the "better satisfaction" at this time does not lend enough likelihood to project profit increase. An intangible cost may be employee resistance to change.

Business Case

The cost-benefit analysis should include only incremental cost. This means existing hardware generally should not be included. However, if the use of existing hardware, premises or management resources would result in another project having to make procurement or hiring, then the cost of such existing resources should be included in the

cost-benefit analysis of the current project. The salary of existing programmers and other staff dedicated to the projects should be included as it varies with project requirements, including the cost of staff members or consultants assigned to the project on a part-time basis. Cost and benefits should be treated on a cash basis; e.g., even though hardware will be depreciated over a number of years for accounting income calculation, the full cash outlay of the purchase should be included as up front cost. The depreciation calculated in income tax returns should then be treated as reduction in cost after applying the income tax rate, i.e., the tax savings from capital cost depreciation should be treated as recurring cost reductions.

Consider the time value of money. Expenses and revenue that occur in future periods should be discounted using the organization's expected rate of return from capital.

Consider the uncertainty of estimates. Future revenue, even if covered by a contract, bears some uncertainty, and should be discounted based on factors such as the customers' reputation and the organization's track record in delivering the products and services. Estimated cost will usually occur, especially costs that are stipulated in contracts. In addition to accounting for the time value of money, future revenue increase should be discounted based on risk. Such discounting should be applied even if future revenue is based on a signed contract, because of the risk of a contract breach. Management should take into account the uncertainty created by new technology and large project size when estimating costs.

External costs that are stipulated in contracts will occur and can be taken at face amounts. Internal costs may be subjective depending on who is doing the estimation. Business units that provide internal services have a tendency to overestimate their costs to insulate against unforeseen circumstances and unfavorable factors beyond their control. On the other hand, project managers and sponsors who feel strongly for a project would tend to lean towards the low end of a range of estimated cost and the high end of estimated revenue. Organizations should expect project managers and sponsors to negotiate competitive costs with internal and external service providers and hold the business units accountable for cost estimates. Decision making with respect to approving the initiation and continuation of a project should involve some discounting of revenue estimates and grossing up cost estimates, except for items that are locked in by contracts with reputable customers and vendors. The factors that should be considered in such discounting and gross-up include:

1. Remoteness of timing - The farther out the timing for estimates, the less reliable they are. For example, for each year out, a 1% discount of revenue and gross-up of cost can be applied. This discount is in addition to the discount for time value of money. It is intended to account for uncertainty related to the time remoteness.
2. Experience with the business and technology - For new ventures and emerging technology, the learning curve makes estimates less precise. Cost estimate should allow for this.
3. Project size - Large projects involve many stakeholders, multiple business units and sometimes different external parties. This increases the difficulty and error margin of estimates, not just in dollars but also in percentage. An organization can set strata of project sizes and apply an escalating rate for discounting revenue estimates and grossing up cost estimates.

The cost-benefit analysis should cover a period of 3 to 5 years, depending on the life of the new system. It should be updated at least annually. Estimates beyond 5 years are less and less reliable.

Treat cost avoidance differently from cost reduction. Cost avoidance constitutes true saving. Cost reduction is difficult to materialize completely. It is easier to avoid giving than to take something back. A common category of cost reduction is expected salary savings. No manager likes to fire people. So even if a department accepts that a new system will reduce the requirement for staff, managers will and should try to find ways to redeploy the surplus employees. However, in doing so, temporary assignments with little value may be created. It is important to take into account the restructuring and retraining expenses in estimating human resources savings that can accrue from using a new system.

Cost avoidance should reflect the new system's ability to prevent adverse incidents. To put a value to such preventive ability, business units should have been recording the costs of incidents. These include:

- Loss of assets
- Loss of revenue
- Legal liability
- Loss of productivity
- Time taken to rebuild systems and information
- Cost of increased paper based transactions during system outage
- Financial resources needed to reassure customers and mend customer relations

At the end of each phase of the project, the risk statement and business case should be reviewed and adjusted as necessary. In the case of cost overrun, the project manager should implement measures to better control costs. Significant variances, e.g., 10%, should be reported to the parties who approved the project proposal to seek a “go or stop” decision.

Project Risk Statement

It is critical to perform risk assessment before devoting resources to develop a system. The proposal should include risk assessment and indication of how the risks will be mitigated. The project risk assessment should consider the common IT risk criteria that are discussed in Chapter Two.

1. Incomplete system implementation – This risk is quite high because there are numerous functions in a system. The main controls to mitigate this are system integration testing and user acceptance testing.

2. Unauthorized system implementation – This risk is also quite high for the same reason. The main control is sign-off of the test results and the conversion plan.

3. Inaccurate system development and implementation – This risk is high. Testing is the main mitigation.

4. Untimely implementation – This can be a common occurrence. The main mitigation includes a detailed project plan and monitoring by the project management office.

5. Implementing a system no one requested (occurrence) – This risk is quite low because a systems development project requires significant resources and if on one asks for the project, it is hard to find the resources. The main mitigation is the requirement for a project plan.

6. Inefficient system implementation – This risk is quite high because of the usually large size of a project and the variety of interfaces required. The main control is management monitoring of the project progress.

The risk of a project increases with the complexity of technology and scope of the project. For example, eBusiness and infrastructure integration projects are of high risk. When an organization conducts an enterprise resource planning (ERP) system project, the risk is very high because of the complexity of the system, the tendency to use consultants owing to lack of internal expertise, the need to manage software vendor relations, business process reengineering involved, changes in business functions, resistance to changes and the wide array of business functions affected.

SYSTEM ANALYSIS

Once the proposal for a solution has been approved, a project is initiated to seek the solution and the business sponsor will designate a project manager. At this time, a small project team should be assembled. The team, consisting of IT and business area staff, should define the project scope by analyzing the existing system to determine the extent to which the problem can be solved with existing system functions. Based on this analysis, the team will assess the extent of the new system and develop a detailed project plan. The result of the analysis phase is a detailed report that describes the effectiveness of the existing system. The following components should be included:

1. System overview in narrative and diagrams.
2. System users.
3. System deficiencies reported in the past. These deficiencies actually are the drivers of the new system.
4. Strong features of the system; these features should be repeated in the new system.
5. Expert developers and expert users of the system. These will be valuable resources in developing the new system.

This report should be signed off by the project sponsor. The next phase is to develop a detailed project plan.

PROJECT PLAN

The project plan should consist of the following.

- Project objectives.
- Project team.
- Business sponsor and project manager.
- Work breakdown structure – This is a detailed list of activities that have to be carried out to develop and implement the system. They are grouped by phase. For each phase and activity, the persons responsible for the work and signing off should be stated. The timeframes should also be stated.
- Time table – It is also called a Gantt chart. It shows the tasks under each systems development phase, timetabled ideally by week, showing the name of each team member responsible for each task during each week, the number of hours needed, as well as the deliverables and checkpoints for approval. Actual progress in terms of time spent and deliverables completed can be shown on the Gantt chart to be compared to the plan.
- Critical path diagram to show the tasks that have predecessors, i.e., a task that cannot start until certain tasks are completed. This diagram will help the project manager to determine the impact of task slippage in terms of the ability to meet the project deadline. The critical path is the path of predecessor dependent tasks that takes the longest elapsed time. Any delay of this path will delay the project; i.e., there is no slack time allowed. This tool allows a project manager to assess the impact of task delay.
- Responsibility of each team member.
- Approvals required.
- Incident notification contacts.
- Detailed risk assessment
- Risk mitigation plan

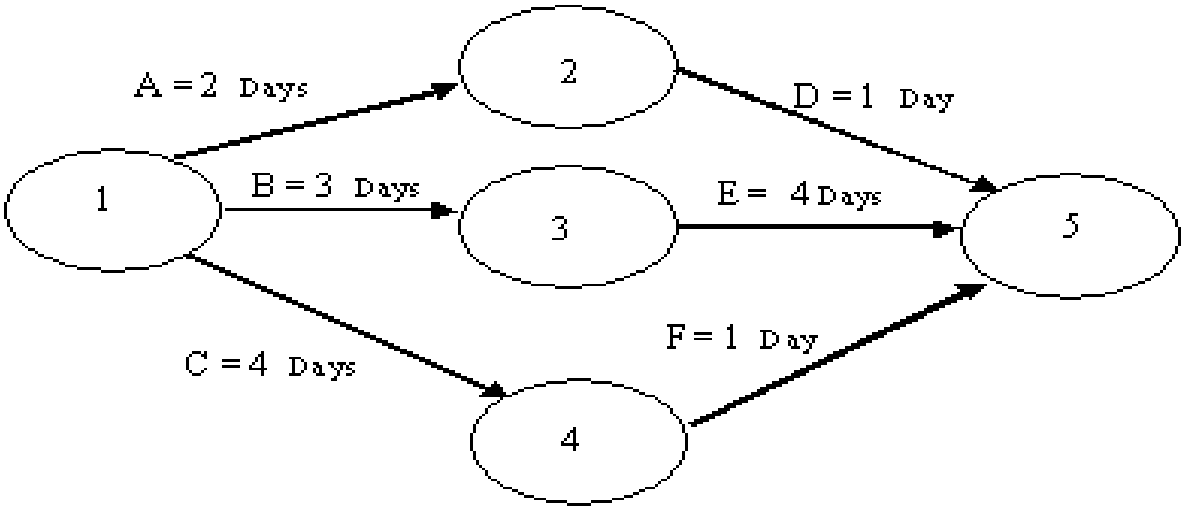
A project management software tool should be used to help ensure comprehensiveness of the project plan, its monitoring and reports. Studies show that the duration of a project should not exceed 3 years, for the following reasons:

- It is difficult to keep the team focused on a project for a longer period.
- After 3 years, the business environment may have changed so much that the solution is no longer competitive.
- Technology may have changed so much that the solution is no longer the best available given the cost the organization is willing to commit to.

The project plan must be signed off by the project sponsor.

Critical Path Diagram

The following is a simple example of a critical path diagram.



This diagram shows that tasks A, B and C are not dependent on each other; nor are D, E and F. The minimum duration of the project is seven days. Any delay in task B or E will delay the project. How about delay in task A? Well, it depends on how much delay. B to E is called the critical path because it is the longest path of predecessor dependent activities in terms of elapsed time, i.e., 7 days. A to D will take 3 days. Thus, A and D combined can be delayed for up to 4 days without delaying the project. A critical path diagram is useful to measure the impact of delay of certain activities on the project's timely completion. Well, if B is delayed, what should the project manager do? S/he should assign more resources to catch up and prevent further delay. If additional resources are not available, stakeholders should be informed and a revised deadline should be negotiated. The project manager should also institute correction actions to prevent further slippage.

Project Team

The project team must be formed before the work stated in the work breakdown structure is carried out. Some team members may be assigned part time to the project from within the organization, some may be seconded full time to the project. Some may be hired as new employees for the project and then transferred elsewhere after the project. Some may be hired as term employees just for the project. Some may be consultants. Where team members are seconded from within the organization, the secondment agreement must cover a long enough period. A tricky arrangement is for someone to be assigned part time to the project. The agreement between the project manager and the line manager who supplies the team member must state the duration, the amount of time each week the person will be available to the project and how conflict in demand will be resolved.

Consultant contracts must be supported by statements of work, statements of deliverables, checkpoints, provision for conflict resolution and corrective action, as well as remedy for non-performance.

Gantt Chart

This is a time table of the project activities grouped by phase indicating the time and deliverables expected of each team member. Project management software can be used to prepare this chart. Over the course of the project, actual time and deliverables can be input to the software and overlaid on the chart to compare with the planned progress. Here is a simple example of a Gantt chart.

	Week 1	Week 2	Week 3
User requirement: First draft	V D'Angelo – 10 hrs	T Cruise – 12 hrs	S Feng – 14 hrs
Second draft	Shashi Ghandi – 5 hrs	B Zhou – 8 hrs	D Cohen – 3 hrs
Sign-off			C McNichol – 5 hrs

Project Management Skills

The Project Management Institute develops education and reference material for project managers. It also grants the Project Management Professional (PMP) designation upon successful completion of a uniform examination and confirmation of meeting the experience requirement. A PMP indicates possession of project management experience and knowledge. A good project manager also needs soft skills.

A project manager has to manage a project team with members who are not assigned to the project full time. When conflicting deadlines or pressure occur, those team members might be inclined to give priority to their full time jobs. Even before that, the project

manager has to identify skilled people from the organization, negotiate their availability and in some way "attract" those people to join the team. Although the project manager can hire people, for cost effectiveness and knowledge availability, an effective project team should consist of a critical mass of existing employees.

A common risk in projects, especially systems development projects, is scope creep. That is, users keep changing their requirements. This can delay project completion. A project manager must be firm and not afraid to say no. User requirements should be frozen after sign-off by the project sponsor unless there is a huge gap. The project manager must also be organized as detailed planning and monitoring are important. The project manager must be knowledgeable about the business, pragmatic, a good listener, a good articulator and have overall knowledge about IT. S/he must be deadline conscious and lead by examples. S/he has to be good in holding and controlling meetings. Too many meetings are too long. Last but not least, the project manager must be good with people, to make people feel good in the head and the stomach. The adages "motivated staff are productive staff" and "respect must be earned and cannot be demanded" apply aptly in project management.

It seems like a project manager has to walk on waters; well, almost. Because it is such a demanding job, successful completion of a major project often will land the project manager a promotion…and the converse may also be true.

Where do project managers come from? Are they hired to run a project, transferred from the IT department or from the business unit? The answer is, it varies. It depends on the type of system, the availability of internal expertise, the technical knowledge required and the urgency. Many successful project managers did not come primarily from the IT area. One can argue that an experienced project manager for a building construction project can run an IT project well. There is more emphasis on management than IT. A large organization should have a project manager pool in the PMO. A project manager may run a large project only or several small projects simultaneously.

Before any system development work can start, the project manager must obtain detailed system requirements from the user area.

USER REQUIREMENTS

This is largely the responsibility of the business area sponsoring the system. Requirements should be detailed. It should state what transactions will be processed and how, what information is required in the solution, when it is required, who it has to be available to. It should also include what system functions are required to be used by whom. User requirements should state the reports and whether they have to be online. The frequency of processing should also be described. The availability of the system in numerical terms should be specified, e.g., 24/7, 99.99%. The requirements should indicate the types and volume of transactions to be processed and the format of the transactions. The requirements should be reviewed by the project manager and the IT department to make sure that they are understandable to the technical people who will develop the system. User requirements should include provisions to comply with the

associated policies and standards. How transactions will be processed includes defining what transactions will be processed online, in batches, centrally, in a distributed manner etc.

For systems that process financial information, the accounting department should review the user requirements to ensure that the organization's accounting principles are followed. The team preparing the user requirements should be aware of the organization's policies and standards that pertain to or address internal controls, to ensure that controls are included in the requirements. It is important at this time to state the information and audit trail that is needed to carry out management review and approval as well as independent checks. The team should also consider the need to refer the requirements to the legal department.

Internal controls should be included in user requirements in two ways. First, they should be integrated in the business process and information requirements. Secondly, they should be pulled out as a separate section. This control section will help people who perform risk assessment to determine the adequacy of internal controls. The user requirements should include both automated and manual functions because the systems developers will need to know how people interface with the system. Even if a manual function requires no system interface, if it uses system produced information, it should be stated so the systems developers know how information will be used and this will help them in designing the system function and data format. The control matrix shown in the last chapter should be used as a frame of reference to compose internal controls that will be built into the system along with manual controls.

	Completeness	Authorization	Accuracy	Timeliness	Occurrence
Input					
Processing					
Output					
Storage					

User requirements should be detailed and account for input, processing, output and storage. Input will include the types of transactions to be processed, what information will be gathered, input form etc. Processing will include the functions to be performed, e.g., aging of accounts receivable in 30 days, 60 days; batch processing vs online processing; centralized processing vs distributed processing. Output should indicate the exact output screens and reports, whether reports will be regular or on demand, who can get what reports, hard copy or electronic, retention of data and reports etc. As far as storage, the user requirements should address where data will be stored, for how long and who are responsible.

The following questions must be addressed, at a minimum, in the user requirement document:

1. What will be recorded? In other words, what is a recordable transaction?
2. How will the transaction be recorded?
3. When will the transaction be recorded?

4. What system related internal controls will be necessary to ensure authorized, accurate, timely, complete and efficient execution and recording of transactions?
5. What system related internal controls will be necessary to ensure that only real transactions are recorded?
6. What input screens will be used?
7. What output and enquiry screens will be necessary?
8. What management and other ad hoc system queries will be necessary and available?
9. What reports will be produced and in what format? Will they be pushed to users or pulled by users?
10. When reports will be produced?
11. Details of each report and system enquiry and their layout.
12. What staff positions will input transactions and receive reports?
13. What staff positions will need to perform which system enquiries?
14. Whether each transaction or enquiry is needed to be input or invoked centrally or in distributed locations, and which locations?

Depending on the system, transactions include financial transactions like invoicing, finance related transactions like setting up a general ledger account, and non-financial transactions like setting up a user access profile.

In developing a new system to replace a current system, the project sponsor should charge the business unit representatives to go through a paradigm shift to streamline processes. A value chain should be established to ensure that each system function and related manual procedure adds value, and that the value added exceeds the cost of developing the function as well as the cost of exercising the function and related activities. This streamlining process is also called business process reengineering.

Here are the common steps an organization should follow in business process reengineering.

1. Build a cross functional team with experts in each business area involved.
2. Identify and agree on the business objectives.
3. Develop a value chain including applying activity based costing.
4. Benchmark the value chain with industry standards as well as known competitors' cost and system performance metrics.
5. Validate the value chain with testing and prototyping.
6. Establish performance indicators for subsequent measurement of the development process and the operational system.

Based on detailed user requirements, system developers can start the technical work. System architecture should be prepared to develop the system infrastructure. Meanwhile, system design can proceed to construct the software and database.

SYSTEM ARCHITECTURE

Based on user requirements, IT architects will define the network topology and required hardware. The documentation will be in diagrams, flowcharts and narrative. It is called system architecture. System architecture is design of the system's infrastructure. The system may well be using existing infrastructure with or without addition. Even if there is little or no new infrastructure, the system architecture has to state that. It should detail how the new system will use the existing or new infrastructure. System architects are experienced and skilled in network design.

They may be former programmers, former software designers, hardware engineers, software engineers or people trained specifically in network management or database administration.

General controls should be included in the system architecture. Examples are firewall, network authentication, virus checking and redundant servers. Application controls are not required here as they will be addressed in system design.

Although the system architecture should be based on user requirements and internal controls should be specified in the user requirements, business unit people are not qualified and knowledgeable to think about the general controls that are usually technical in nature and are not directly tied to a transaction cycle. For example, users would not know whether a firewall is necessary. It is therefore important that system architects be trained in internal control concepts and techniques. System architecture must comply with the organization's policy and standards about hardware and system software configuration, e.g., security parameters. There should be a standard checklist followed by the architects. Because many infrastructure controls are of a security nature, it is important for IT security specialists to participate in this process.

The system architecture should be signed off by the project manager, the IT department including the programming manager, user representatives, system designers, internal audit and IT security.

SYSTEM DESIGN

Based on the user requirements, the assigned IT staff members can design the software solution. The design should address the following.

- The input to be processed, including what data is required, the format, who it comes from, frequency, whether it is in batches or online.
- The edit and authorization checks to be performed on the input.
- The computerized processing functions, their sequence, frequency, input and output.
- The computer checks to be performed on processed data and results.
- The format of reports and whether they are online or in hard copy.
- The format of input and whether they are in batches or online.
- Whether reports are automatically sent or produced on request.
- The information needed for management and staff to perform review, checks, approval and reconciliation.

- The format, size and media for databases and files.
- The software tools required.
- Interfaces with external entities.

Design documentation will take the form of entity relationship diagrams (ERD), data flow diagrams (DFD), flowcharts, data dictionary, input screens, forms, report layouts and narrative. Application controls should be included in a more detailed form than those in the user requirement document. There should be cross-referencing of the system logic to user requirements. There are software engineering tools to draw the diagrams. The designers must review such diagrams for consistency with the user requirements.

System design must comply with the organization's policy and standards about hardware and system software configuration, e.g., security parameters. There should be a standard checklist followed by the designers.

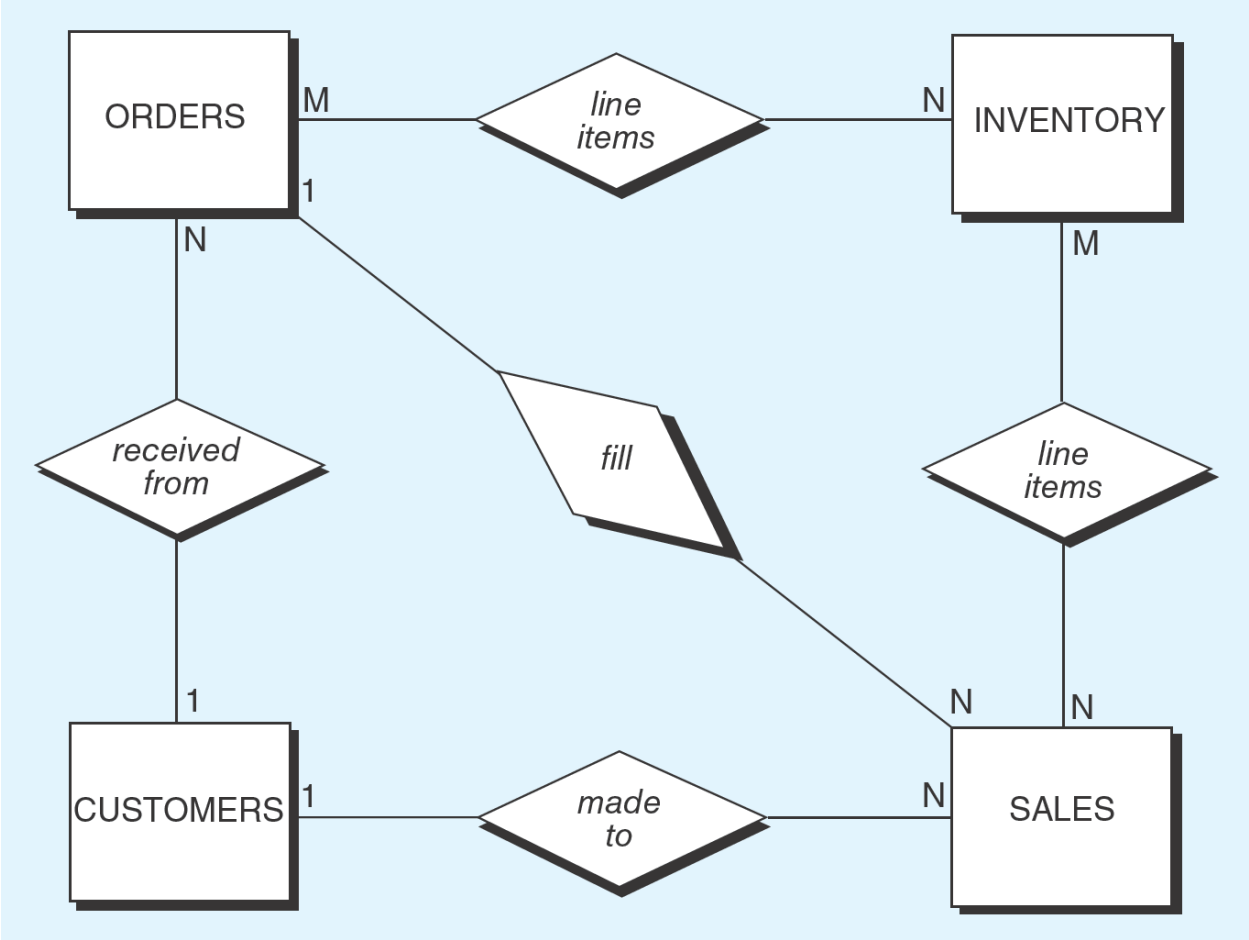
The final deliverable of the design phase is pseudo code. This is a set of system processing activities almost in the form of computer programs. This is why it is called pseudo code. Some people call it programs in plain language. It is somewhat less detailed than computer programs, especially in input, output and data storage tasks. Programmers will write programs based mainly on pseudo code. They will use narrative and diagrams described above as secondary references.

The design documentation package should be signed off by the project manager, user representatives, the programming manager, the assigned IT architects, internal audit and IT security.

Entity Relationship Diagram

Before system logic can be worked out, the designers should review the user requirements and understand the external and internal entities in a system. Examples of external entities are customers and banks. Examples of internal entities are departments.

An entity relationship diagram (ERD) shows the relationships between entities. The relationships is usually expressed in actions. The following is an example of an ERD. The top level ERD should show all the external entities and the major internal entities.



The above diagram shows the relationships and cardinalities. For example, a customer order may contain multiple inventory products and vice versa. Such a table is useful to design database tables. Each entity should be depicted with a table. The cardinality will be useful to define the linkage between primary keys and foreign keys. A primary key is one or a collection of contiguous fields that can unique identify each occurrence (record). A foreign key is a primary key in another table but a non-key field in the current table and must not be blank. For example, a customer order must have inventory products. We will discuss this in more detail in Chapter Six.

There are usually multiple ERDs in a system, in successive levels of details. Once the relationships of entities are defined, the designers can compose the database structure and select the database management system. The database structure will include the following:

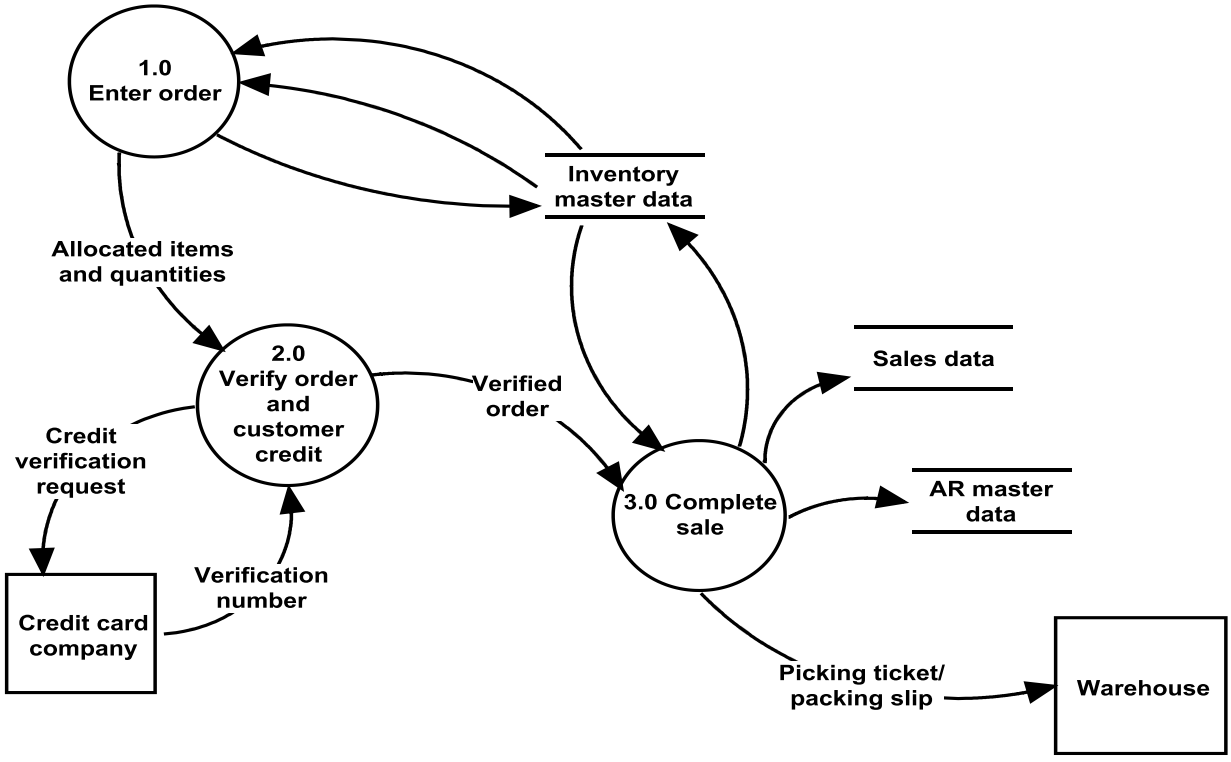
- A data dictionary that defines how data is stored in each table and in what fields, data format, field lengths and order. There should be a table for each entity. Some entities have successively detailed tables.
- Database management system.
- Table layout.
- Table relationships.

- Access control lists defining which computer programs have access to which tables and which fields and the nature of access, e.g., read, update, delete.
- Database schemas, i.e., logical views for the application that define what each system function and user can access.
- The input forms, manual or online, to collect the data.

We will discuss database management systems in more detail in Chapter Six.

Data Flow Diagram

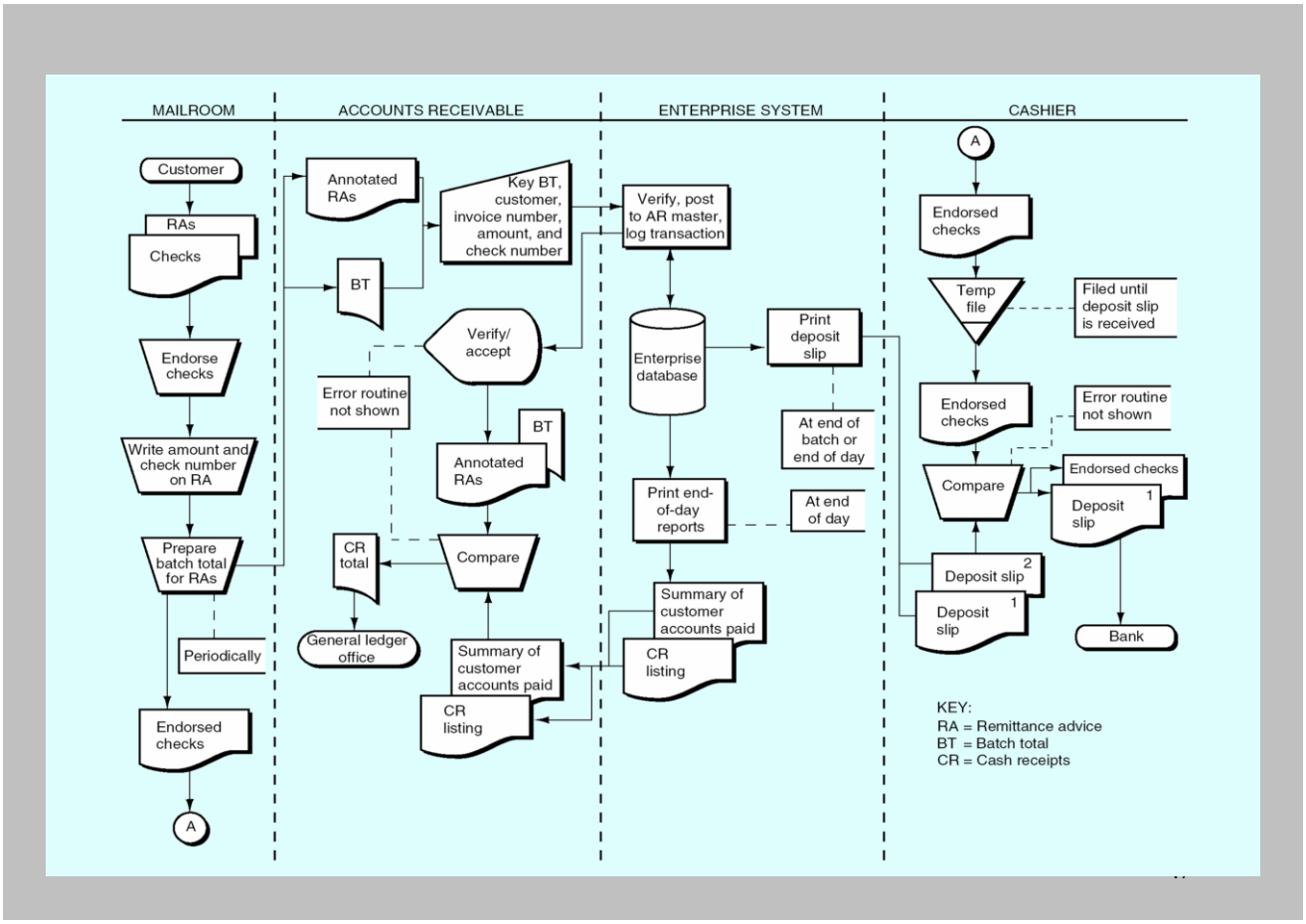
After defining relationships, the designers should study how data should flow between entities to satisfy user requirements. This includes defining the processes. Such definition should be in the form of narrative, data flow diagrams and flowcharts. For each relationship as defined in an ERD, there should be a physical DFD, that depicts internal entities which are parties to each relationship. For each physical DFD, there should be multiple logical DFDs that define the processes by explaining the actions. The following is an example of a logical DFD.



Flowchart

A logical DFD does not describe all system functions and procedures in sufficient detail for programmers and procedure writers to follow. To provide the necessary details, flowcharts are prepared. Many of the procedures in a flowchart are internal controls, e.g., checking to see if a credit limit is to be exceeded. Here is an example of a

flowchart.



Although the system design should be based on user requirements and internal controls should be specified in the user requirements, business unit people may not be knowledgeable to think about the technical IT application controls such as database normalization and referential integrity checks. We will discuss these controls in Chapter Six. It is therefore important that system designers be trained in internal control concepts and techniques like the above, as well as security techniques like boundary checking of user inputs to prevent code injection and buffer overflow by hackers that can distort or misdirect system processing. Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to the assigned buffer of real memory is within the boundaries of that buffer.

Designers should use narrative to supplement the diagrams because the diagrams show the interfaces between processes but do not describe the processes in detail in terms of the system functions including internal controls. The narrative includes two levels. First in point form, it expands the user requirements to account for data layout and data table relationship, and also to describe the entities, documents and processes indicated in the diagrams. A question is, why bother repeating the information in the diagrams in the form

of narrative? Diagrams provide an overview for programmers to understand the relationships between entities and processes. It is easier to use narrative to capture in more specific terms all the relationships and processes, so narrative should be cross checked to diagrams.

The second level of narrative is called pseudo code. It is in the form of program instructions but in plain English. This is actually the final reference source for programmers to write programs. Pseudo code is more detailed than the first form of narrative because it includes technical statements about how data is read and updated. However, during programming, the programmers will find it useful to also study the diagrams when they have doubt about the pseudo code and also to debug programs. Debugging means working out program bugs that cause a program to malfunction. Pseudo code is less detailed than actual computer programs because it covers only input, processing and output. It does not specify data format, the form of input (manual or online) and the form of output.

The design documentation should be signed off by the project manager, the IT department including the programming manager, user representatives, system architects, internal audit and IT security. Internal audit should assess the adequacy of data format for computer assisted audit techniques. The design phase and the architecture phase can be carried out concurrently. However, during construction, the two teams should exchange information and material to ensure that they are compatible, i.e., the infrastructure will support the software.

PROGRAMMING

Once a system solution has been designed, programming can start. A team of programmers will divide the functions to work on, as assigned by the programming manager. There should be a standard for program documentation, testing and naming. Each programmer should test his or her own programs one at a time and in a series. They should also swap programs for peer testing, as assigned by the programming manager. Where existing programs are needed to be used as the basis for change, programmers should apply to the change control coordinator for a copy of the programs that are used in operation, to ensure that changes are made from the current version. Programming is performed in the programmers' own libraries. Peer testing, also called string testing, is carried out in the development library, which is a library with common access by programmers in the project for read only. The systems development methodology should provide guidelines for constructing test cases which should be based on the system design documentation. There should be cross referencing of the test cases to the system design documentation. Every system function should be tested and all linked functions should be tested together.

The IT department should have a standard test bank for each application to ensure consistency of test data. The test bank should be updated periodically to reflect the comprehensiveness of real transactions. Testing for a system development project is more extensive than testing ad hoc program changes. Test results should be signed off by the programming manager and the project manager.

Software engineering tools can be used for code generation for routine functions. The configuration of these tools must be approved by management to ensure consistent coding conventions and documentation. The code generated must also be reviewed by the programmers with written indication of such review to ensure correctness. The use of objects (reusable code) should be subject to risk assessment and management approval to avoid blindly using previously written code. The project management office should maintain an inventory of these common objects and periodically test them.

Open source tools should be subject to the same level of due diligence as reusable objects and should be tested to the same rigor as locally developed programs. The organization should have a policy in adopting open source with respect to approval, types of application allowed, inventory and license violation. The time involved in adapting open source code should be tracked to assess the savings vs developing proprietary code. Open source means ready made programs in source code format available from vendors, trading partners or the IT community.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to the assigned buffer of real memory is within the boundaries of that buffer. Java automatically checks for boundary overrun so is a good language to avoid buffer overflow.

Programming standards and training should specify techniques to avoid security holes being programmed that will open back doors to hackers. For example, an input program must check the validity and length of values input to prevent buffer overflow (overflowing the real memory in the computer and therefore overwriting program instructions loaded in real memory that could then cause a system to misbehave or shut down). Programming standards and training should also address how each operating system service (function) or port is used in the system, in which programs and how these operating systems features are also used in other systems to assess the risk of system compromise if these components are abused by programs or hackers. A port is a channel used for computers on a network to exchange information for a particular application; an example of an application is a network game. A port is analogous to a radio channel.

Reusable code has to be periodically tested and traced to its source version. The source version should then be checked for changes and such changes should be reconciled to management sign-off. Reusable programs should be grouped by functionality and classified in terms of their sensitivity. Management approval should be required to reuse sensitive and powerful programs, in light also of the sensitivity of the application where reusable code will be imported to.

Programmers should be trained and instructed to use ample narrative within programs to make program instructions understandable to the authors and other programmers in the future to facilitate program updates. Narrative can be inserted in line within programs with suitable prefixes so the compiler knows that the narrative is not part of program instructions.

Program flowcharts should be prepared for each system process before actual coding (programming). This helps ensure that programs are written to comprehensively and efficiently meet the system design specifications.

Tested and completed programs should be approved by the programming and project managers. How about user representatives? Shouldn't they sign off? Well, they most likely cannot read programs and so cannot sign off. Don't worry. They will get their chance to test the programs and sign off the system, as stated below. It is true that programming managers and the project manager also probably cannot understand programs. Why bother asking them to sign off? Well, there should be management sign off of this important phase of systems development. Programming managers will sign off on the strength of peer testing and general review of program documentation including program narrative. The project manager will sign off mainly on the strength of the programming managers' signoff. It is not rubber stamping. It is accountability. The project manager should sign off the completion of each phase.

Programmers who worked on a systems development project should not be assigned to perform ad hoc program changes that are discussed in the last chapter, in order for fresh eyes to assess the programs' correctness and detect fraudulent code.

SYSTEM INTEGRATION TESTING

It seems that one can never test enough, as soon as a system is implemented, bugs are discovered. The organization should have standards that guide in determining the extent of and responsibility for testing and how tests should be documented. In addition to testing done by programmers, the system should be tested by independent staff members, who are normally in the IT department but not programmers. It is important for non-programmers to do most of the testing so that they can be objective and think beyond the programs.

Testing must be done in a separate environment without being part of programming and operation. The programs being tested must have strict access control to avoid changes being made after testing without the knowledge of the tester, as that could invalidate the test results. Testing must be thoroughly documented. There are more test cases and extensive test data compared to string testing. That's why this phase is called integration testing.

System integration test result should be signed off by the IT department, project manager, user representatives, internal audit and IT security.

USER ACCEPTANCE TESTING

After system integration testing, user representatives will perform their own testing. This will also include using operations procedures along with system testing and assessing the system's user friendliness and capability to process fluctuating transaction loads. User acceptance testing should focus more on user friendliness and procedures because automated functions have been extensively tested under system integration testing.

User acceptance test result should be signed off by the IT department, the project sponsor, user representatives, the project manager and internal audit.

SOFTWARE CERTIFICATION

Some programs are not just parts of an application. They are reusable code (program source or object code that can be used in other systems development projects) or utility programs (programs that can be used for housekeeping including critical and common functions like backup and archive). In addition to user signoff, these programs should receive certification in the organization for reuse. The criteria for certification should be broad yet detailed, broad in a sense that they take into account the needs of the organization across business units, detailed in that they are rigorous in terms of the extent of testing and documentation. Certification should be signed off by the project manager of the project that creates the reusable code and also by the PMO which maintains a repository of reusable code.

PROCEDURES DEVELOPMENT

Before system implementation, procedures should be developed or updated. These procedures should include:

- User procedures;
- System administration procedures;
- Accounting procedures;
- Technology infrastructures procedures;
- IT security procedures including user account management;
- Technical support procedures; and
- Data and program backup procedures.

Procedures can be developed once the user requirements are signed off. Procedures should be signed off by the user area representatives, project manager and internal auditors.

Procedures should be restricted for access by the intended users of the procedures to prevent breach of segregation of duties. Also, system design and program documentation should be kept away from systems administrators in order to support segregation of duties; e.g., the system administrator supporting development servers are not assigned to also support production (operation) servers.

DISASTER RECOVERY PLAN UPDATE

You can recall from the last chapter that a disaster recovery plan (DRP) should contain a list of business critical systems to be recovered when the backup computing facility is activated. This list will change from time to time depending on business changes, new systems and system retirement. The DRP should be reviewed for every systems development project and updated accordingly.

TRAINING

Training is often put to the backburner. The risk is that systems are designed properly but improperly operated and used. Before system implementation, training material and a training plan should be prepared. Training sessions should be conducted for operators, technical support people and users. The affected active employees should be required to be certified as trained.

CONVERSION AND IMPLEMENTATION

In most cases, data conversion is necessary before system implementation. Conversion should be planned and tested. Data conversion often is automated and the programs that convert data should be subject to rigorous testing. Implementation should usually occur immediately after conversion to avoid the need for multiple conversions. The following are common approaches. There should be a conversion plan. Conversion result should be reconciled to the source files to ensure accuracy and completeness. There are a number of risk based conversion approaches. It is the project manager's decision as to which approach to take. The decision will be based on the complexity of the system, tightness of deadlines and experience with the individual approaches etc.

Direct Cutover

All data from the old system is converted to the new system and the old system stops at the time the new system kicks in. This approach is quite risky because if the new system does not work properly, there will be service disruption and may be data loss. Customer impact could be significantly felt. However, technology advancement and competitive pressure continue to make this approach appealing. Technology advancement can make the fall back arrangement almost seamless; i.e., if the new system has a major glitch, processing can be automatically reverted to the old system. This approach is also called the big bang method.

Pilot Implementation

When the deadline is not tight and the risk of direct cutover is too high considering the complexity of the system, an organization may adopt a more conservative method of conversion and implementation. One such method is pilot implementation. Under this method, a small business unit, e.g., a branch, is selected for using the new system. This is a good way to test the water in a real environment. If the system does not work properly, the damage is limited.

Parallel Implementation

This is the safest implementation method and also the most expensive. It involves running the old system in parallel with the new system. Everything is processed twice. It is costly and impractical for customer service systems. A modified version is to run only the backroom processing in parallel. That would lower the cost and inconvenience but

also would provide less redundant safety margin as fully parallel conversion. Parallel conversion is more practical for accounting systems especially the general ledger systems where there is no customer interface, the transaction volume is low and the required degree of integrity is high. It is also more commonly used for a payroll system which tends to process transactions on a batch basis and there is no customer interaction. Parallel implementation is impractical for an online system because of the inconvenience posed to online business operation where time is of the essence.

Phased Implementation

This is similar to the pilot approach except that instead of selecting a unit to use the new system, the entire organization will use it but only selected functions will be turned on, and those corresponding functions of the old system will be turned off. If the replaced functions of the old system cannot be turned off, transaction adjustments will be made for the overlap, and that can be complicated.

Conversion and Implementation Plan

The conversion and implementation plan should include the following:

- Old file names and versions to be converted.
- Names of new file and system versions.
- Dates of conversion and implementation.
- Approach (method) to conversion.
- Programs used to convert.
- Procedures and responsibilities.
- Tests to ensure completeness and accuracy.
- A checklist to ensure people, infrastructure, software, procedures and information are ready and have been implemented.
- User signoff.

The conversion plan and result should be signed off by the IT department, project manager, user representatives and internal audit.

POST-IMPLEMENTATION REVIEW

Every system should be subject to a post-implementation review. The purpose is to assess whether the project is a success. Some projects might have finished on time and on budget but the systems are not useful. The review should be done 3 to 6 months after implementation by someone who did not develop the user requirements, perform testing or take part in other system development work for the project. Quite often, an internal auditor is a suitable person. The review should entail interviews with users, control walkthrough, assessing whether the activities in the project plan have been carried out properly and assessing whether the business case was adhered to. Detailed project documentation will be reviewed. The review report should indicate the following:

- Total project development cost compared to budget cost.
- Any user requirements not included in the system or not functioning properly.
- Missing project documentation.
- Missing approval of project deliverables.
- Summary and details of user feedback.
- System and project management deficiencies.
- Recommendations for corrective actions for the current project and improvements for future projects.

Post-implementation review should be conducted by people independent of systems development and management for the project. Internal auditors and quality assurance staff members are often desirable candidates to carry out this review because of their objectivity. The report should be addressed to the system sponsor. Ideally, internal auditors who were not involved in the systems development audit in terms of reviewing project documentation during development should perform the post-implementation review. If such "independent" auditors are unavailable, even auditors who reviewed the system documentation during development are still reliable to perform the post-implementation review because they can draw on their knowledge gained during the project and also because auditors are trained to be objective.

Project or system deficiencies should be corrected immediately to the extent practical. For example, if certain sign-offs are missing, the responsible stakeholders should provide the sign-off even if it is tardy, such as a programming manager's sign-off, in order to complete the project documentation and acceptance of accountability. Another example is inadequate testing or training. Such findings should also be corrected as soon as possible. Some findings, however, are meaningless to correct retroactively. For example, if project meetings were held only monthly instead of bi-weekly as called for by the project plan, there is no point in holding the missed meetings because the project is done. A recommendation to address this would go along the line of strengthening future assurance that project meetings are held on a timely basis, by perhaps implementing an email notification to the project sponsor with meeting minutes bi-weekly.

SUMMARY OF SYSTEMS DEVELOPMENT AND ACQUISITION PHASES

1. At an organizational level, develop a three year systems development plan that is updated every year. This is part of the IT strategy. The systems development plan should include all current and planned projects. The start dates, checkpoints, end dates, deliverables and resource requirements should be included for each project. The CIO is responsible for this and the IT steering committee should approve. Internal and external auditors should be informed. The project management office should maintain this plan.

2. Problem recognition, which is a business unit responsibility, must be approved by the system owner(s) of the systems to be replaced and developed, before the development of each system.

3. Feasibility study, a business unit responsibility, must be approved by the system owner(s) of the systems to be replaced and developed, before the development of each system.

4. Project proposal, a business unit responsibility, must be approved by the level of management with financial authority to sign off the net cost of the project over the life time before netting the cost with operational savings. Operational savings may not materialize if circumstances change or the estimates are too liberal. Before being approved by senior management for funding, the proposal should be signed off by project sponsor, CIO, CFO and internal audit.

5. System analysis, a project manager responsibility, must be approved by the project project sponsor.

6. Project plan, a project manager responsibility, must be approved by the project sponsor and IT department. Internal audit should also sign off.

7. User requirements, a business unit responsibility, must be approved by the project manager, IT department and project sponsor; should be signed off by internal audit and IT security. The IT architecture and design units must also sign off to make sure the user requirements can be expanded to architecture and design specifications.

8. System architecture, an IT department responsibility, must be approved by project manager. It must be signed off by the lead designer, internal audit and IT security. It is not necessary to have project sponsor signoff because of the technical nature of the material and it is a less major milestone than user requirement definition.

9. System design, can be carried out concurrently with system architecture, is an IT department responsibility. It must be approved by project manager, user representatives, project sponsor, system architects, internal audit and IT security.

10. Programming, an IT department responsibility, must be approved by the programming and project managers.

11. System integration testing, an IT department responsibility, must be approved by project manager and the IT department. It must also be signed off by internal audit and IT security.

12. User acceptance testing, a business unit responsibility, must be approved by the project manager, IT department and project sponsor. It should be signed off by internal audit.

13. Procedures development can be carried out concurrently with the above processes after system design. This is a project manager responsibility. It must be approved by the project manager and IT department. It should be signed off by internal audit.

14. Disaster recovery plan update, an IT department responsibility, can be carried out concurrently with the above process after system design. It must be approved by project manager, IT department, project sponsor and internal audit.

15. Training can be carried out concurrently with the above process after system design. It is a business unit and IT department responsibility, it must be approved by project manager and project sponsor. Affected active users and support staff should be internally certified.

16. Conversion and implementation, a project manager responsibility, must be approved by the IT department and project sponsor. It should be signed off by internal audit.

17. Post-implementation review is a project sponsor responsibility. It must be signed off by the CIO, internal audit and the project manager. The review should be done by someone independent of the systems development project.

MANAGEMENT CHECKLIST

1. Develop a systems development methodology that addresses systems development, systems acquisition and rapid application options.

2. Develop an end user development policy.

3. Ensure internal audit, business areas, CIO and IT security are involved in systems development.

4. Set procedures to inform the board and the IT steering committee about major projects.

5. Ensure that IT staff and appropriate user areas are trained on the systems development methodology.

6. Develop an annual systems development plan containing planned and active projects.

7. Establish a project management office to monitor and report on systems development projects.

8. Develop quality assurance metrics and procedures for systems testing, documentation, training and acceptance.

9. Establish a business case methodology as part of the systems development methodology that is consistent with corporate policies.

10. Prepare quarterly status reports on active projects measuring progress, cost and benefits.

CONCLUSION

Systems development is a major IT activity in most organizations. Even organizations that use purchased software packages often find the need to enhance the systems' functions or tailor the packages to their environments. Systems development may seem straight forward in that users are free to define their requirements and the IT department is expected to write programs to fulfill the requirements. In fact, it is a risky undertaking because of the need to coordinate expectation and understanding between users and stakeholders who may not be IT savvy and because of the increasing interaction between systems in today's globally competitive environment. Many organizations have failed to complete systems development projects and have produced the wrong systems in relation to their business needs. Organizations need to mitigate this risk by implementing a systems development methodology to be used consistently to ensure that the development of only duly requested systems is authorized, accurate, efficient and complete and that implementation is timely.

REVIEW QUESTIONS

1. What are the different phases of system testing and who are involved?
2. If an organization hires a firm to develop a system, how does the organization ensure that the system will be maintainable, i.e., changeable?
3. What are the pros and cons of buying a system?
4. What is a good use of the critical path diagram?
5. Who should sign off the user requirements and why?
6. When should internal controls be first included in a systems development project?
7. Who should the project manager report to?
8. Write a job advertisement for a project manager.

CASE #1 - Internal Audit Report – Agriculture and Agri-Food Canada

For the following excerpt of an audit report on National Land & Water Information Service Project - System Under Development, of the Canadian Government, prepare an audit program that includes at least ten audit procedures that you think the audit team has used. Show the objective of each procedure. Do not be restricted by the findings and conclusion in this report.

Audit Report - National Land & Water Information Service Project - System Under Development Audit

Office of Audit and Evaluation
October 2008

Table of Contents

1.0 Audit Objectives

The overall objective of this "System Under Development" (SUD) audit is to provide management with independent assurance on the adequacy and effectiveness of key elements of the control framework for the National Land and Water Information Service Project (the "NLWIS Project" or "Project"). A SUD audit is a parallel or concurrent review of the relevant System Development Life Cycle (SDLC) stages of a project, as they are happening, to highlight risks/issues and provide necessary risk mitigation recommendations to the appropriate management.

During the audit planning phase, three risk areas and specific audit objectives were identified:

Project Governance: Assess project governance to ensure it demonstrates evidence of a well-defined structure of roles, responsibilities and authorities within which the Project operates, and within which all major decisions concerning the scope and objectives of the Project, including changes, are made.

Business Requirements: Assess the adequacy and efficiency of processes implemented to define, record, update and manage business requirements in support of development efforts and the delivery of business solutions identified in the Project's business case.

Project Management: Determine whether NLWIS project management practices, processes and controls are consistent with industry best practices and relevant government and departmental policies.

2.0 Scope and Approach

Like any system in its development phase, the NLWIS Project environment is constantly changing as project activities, objectives, risks and controls evolve to reflect the stage of the Project, lessons learned and stakeholder needs/input and other changes in the operating environment. It is important to note that this audit reflects an assessment of project risks and controls during a specific period of project implementation. To the extent possible and to ensure relevance of audit findings, audit procedures were tailored to take account of the state of NLWIS project development.

The audit of the NLWIS Project was included in the Office of Audit and Evaluation's approved 2007-08 Internal Audit Plan. Audit planning began in June 2007 and culminated with the completion of a risk assessment and audit plan in October 2007. Audit field work, which included a review of key documents, process walkthroughs, limited substantive testing and extensive interviews, was conducted during the period

November 2007 to January 2008. Synthesis and analysis of findings took place in February and March 2008. The audit was conducted with the assistance of professional staff from PricewaterhouseCoopers LLP.

Auditors were provided with unrestricted access to project documentation and personnel. We wish to express our appreciation to NLWIS management and staff for their assistance and cooperation in providing documentation and participating in interviews throughout the course of this audit.

The following chart outlines the three phases of the audit approach and key tasks within each phase:

Approach of NLWIS SUD Audit		
Phase 1 Planning Jun 07-Oct 07	**Phase 2 Fieldwork Nov 07 - Jan 08**	**Phase 3 Analysis & Reporting Feb 08 - May 08**
Project Initiation. Kick-off meeting. Obtain documentation. Develop interview list. Scan Document Interviews Conduct preliminary interviews Review key managerial controls and risk management processes. Risk assessment. Develop detailed audit plan and schedule.	Conduct audit program using the following techniques. Interview project personnel. Review documentation. Conduct process walk-throughs.	Analyze findings & synthesize issues. Prepare audit observations. Validate findings with management. Prepare draft audit report. Prepare final report with recommendations. Finalize all audit working papers. Obtain and review management response and action plans.

Audit criteria for this SUD audit were drawn from the following sources:

- COBIT (Control Objectives for Information and related Technology), a set of best practices for information technology management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI);
- Treasury Board's Policy on Management of Information Technology (MIT), which promulgates the efficient and effective use of information technology to support government priorities and program delivery, increase productivity, and enhance service to the public;
- Treasury Board's Enhanced Framework for the Management of Information Technology Projects, which is designed to ensure that information technology projects fully meet the needs of the business functions they are intended to support, deliver expected benefits and are completed within their approved schedule, cost and functionality.

Sufficient audit work was performed and sufficient evidence gathered to support the conclusions contained in this audit report.

3.0 Background

The NLWIS Project is a $100 million Major Crown Project. Treasury Board's Policy on the Management of Major Crown Projects states that a project is deemed to be a Major Crown Project when its estimated cost will exceed $100 million and TBS assesses it as high risk.

The purpose of the NLWIS Project is to transform the way the Department of Agriculture and Agri-Food Canada (AAFC) uses geomatics by rationalizing the Department's geomatics investments (people, data, infrastructure, IT applications, services and management), and rolling these into an enterprise service.

NLWIS's cross-functional and geographically dispersed team has presented some challenges.

A project priority was to provide on-line access to detailed information about land, soil, water, air, climate and biodiversity using a combination of geospatial and business intelligence technologies. Information made available by this service will be developed in concert with other federal departments, provinces and territories and allow land managers to access multiple geospatial information services through a single web portal. The end product is an effective decision support tool to help local, regional and national land-use planners and managers assist the Canadian agricultural sector in making effective land management decisions.

The NLWIS Project lifecycle is comprised of the following phases to be implemented over the period from 2005/06 to 2008/09:

- Phase I: Single Window (build a new single Internet portal for applications, data and tools currently situated in various Web pages on the AAFC Online Web site);
- Phase II: Geographic Environment (build the infrastructure, procedures and processes for the new AAFC Geographic Information Services (GIS) enterprise system);
- Phase III: National Source for Agri-environmental Geospatial Information (provide national direct access to geospatial data, spatial functions and additional functionality through improved technology); and
- Phase IV: Integration of Information from Collaborating Organizations (develop new software tools and updated and standardized databases in order to provide value-added information, products and expertise for land-use decision support).

During the audit conduct phase (November 2007 to January 2008), the NLWIS Project was in its third year of development, with just over a year remaining in its lifecycle.

4.0 Audit Summary

The NLWIS Project is technically complex (i.e., cross-functional with a geographically dispersed team), involves many stakeholders from within and beyond AAFC, and has a $100 million budget.

This SUD audit assessed Project risks and controls during a specified period of time. Audit fieldwork occurred in year three of the Project life-cycle, November 2007 to January 2008, just prior to the NLWIS Executive Director's proactive initiation of a review of the overall health of the Project, followed by an aggressive 13-month action plan to address its findings.

Given the magnitude, complexity and stage in the NLWIS Project lifecycle, auditors expected to see and confirm a relatively mature control framework and a system development control infrastructure in place that reflects industry best practices and meets Government of Canada requirements.

Audit findings in the next section of the report are presented on an exception basis. That is, findings describe areas of weakness in the project controls that were examined in the course of this audit.

Notwithstanding the findings and recommendations within this report, the audit team found a number of areas of strength in the controls and control environment, in particular:

- The use of appropriate System Development Lifecycle (SDLC) Techniques;
- Consolidation of testing under a single manager;
- A focus on continuous improvement including a management-led review and follow-up action plan for the final year of the Project, "lunch and learn" sessions and "way forward" documents;
- Evolving governance structures to strengthen decision-making and accountability; and,
- Establishment of a Change Control Board which represents a significant enhancement to the change management process.

However, audit findings also indicate that, although there is evidence of improvement since the Project's start, during the time of the audit, established controls for project governance, business requirements and project management did not yet reflect the expected level of maturity nor industry best practices.

While management had initiated action on many of these issues at the time of the audit, there are a number of challenges that require attention. Unless addressed, these challenges increase the risk that the Project will not achieve one or more of its objectives related to value-for-money and/or service sustainability in a timely manner.

Challenges identified by the audit are summarized below:

Project Governance

- Steering Committee function and membership does not reflect best practices in terms of membership and stakeholder representation.
- Incomplete and/or dated documentation of roles and responsibilities of governance committees, project resources and stakeholders which has led to instances of confusion and inconsistency between observed and expected roles.
- Based on project organizational charts, the Quality Assurance function does not have the expected autonomy and independence.
- Duties amongst teams responsible for application development, architecture and business requirements are insufficiently segregated.

Business Requirements

- Business requirements are not effectively gathered and systematically prioritized within a sound governance framework. Specifically, business requirements are not:
    - independently validated by the Quality Assurance function;
    - clearly linked to user requirements or work breakdown structures; or
    - linked to architecture/application designs or release deliverables that had been developed with active participation of key stakeholders.

- As of November 2007, the Project's business requirements document had not been validated or signed off by stakeholders.

Project Management

- The Project's change management process has compliance issues.
- The Project's risk management process was not effective throughout the Project lifecycle.
- The Project had limited capability to track and assess value-for-money as project reporting did not link expenditures to realized benefits.
- There is limited capability to forecast whether the Project will be delivered on time and within budget.
- There has been limited focus on planning for project completion and transition to the end-state.

It is important to note that this audit was conducted at a time of significant change in the senior management level of the NLWIS Project. Subsequent to the audit, proactive measures were taken to assess Project gaps and weaknesses and implement corrective measures. Nevertheless, sustained attention and further enhancements are required as the Project enters its final year.

5.0 Conclusions

Based on the audit findings, significant control weaknesses exist in the areas of project governance, business requirements and project management. Such weaknesses pose serious risks to the timely achievement of the NLWIS Project objectives and therefore require immediate attention to ensure successful project outcomes.

CASE #2 – Shasha Corp.

Jackie Tanaka was hired six months ago as the controller of this mining company headquartered in Toronto, Canada. Before working at Shasha, Jackie was the controller of a petroleum company, Amazing Oil Company, based in Singapore. The joint interest billing and fixed asset accounting systems of Shasha are outdated, and many processing problems and errors have been occurring quite frequently.

Tanaka immediately realized these problems and informed the president, John Kern, that it was crucial to install a new system. Kern concurred and met with Tanaka and Sally Kurek, the CIO. Kern told Kurek to make the new system a top priority.

Kurek left the meeting feeling overwhelmed because the IS department is currently working on two other very big projects, one for the production department and the other for the geological department. The next day, Tanaka sent an email to Kurek indicating the name of a system he had 100 percent confidence in - Good Find - and he also indicated

that he would very much like this system to be purchased as soon as possible. He stated that the system had been used with much success during the past four years in his previous job.

Due to the urgency demonstrated in the meeting with the president and the overworked systems staff, Sally decided to go along with Jackie's wish and sent only a request for proposal out to Wondersoft, the developer and sole vendor of Good Find. Wondersoft responded with a quotation. The purchase price ($175,000) was within the budgeted amount. Sally contacted the two references provided and was satisfied with their comments. Further, she felt comfortable since the system was for Jackie's department, and he had used the system for four years. The plan was to install the system during the month of July and try it for the August transaction cycle. Problems were encountered, however, during the installation phase.

The system functioned very slowly on the hardware platform owned by Shasha. When Sally asked Jackie how the problem had been dealt with at Amazing Oil, he replied that he did not remember having had such a problem. He called the systems manager from Amazing and discovered that Amazing had much more powerful servers than Shasha. Further investigation revealed that Shasha has more applications running on its servers than Amazing did, and that Amazing had a load balancing network.

It was also noted that the data transfer did not go smoothly. A few data elements being stored in the system were not easily retrievable. Kurek found that the staff at Amazing was very friendly when she called, but they could not always identify the problem over the phone. They really needed to come out to the site and investigate. Tanaka was surprised at the delay between requesting an Amazing consultant to come out and the time in which he or she actually arrived. The system finally began to work somewhat smoothly in January, after a grueling fiscal year-end close in October. Tanaka's staff viewed the project as an unnecessary inconvenience. Two accountants quit. The extra consulting fees amounted to $155,000. Further, the systems department at Shasha spent 500 more hours during the implementation process than it had expected. These additional hours caused other projects to fall behind schedule.

Required

Discuss what could have been done differently during the design phase. Why were the problems encountered?

RUNNING CASE – Blackberry

How do you think Blackberry has applied the systems development methodology discussed in this chapter to its Blackberry 10 development. Describe each phase and what could go wrong in relation to Blackberry 10.

MULTIPLE CHOICE QUESTIONS

1. A company has hired a consulting firm to develop a system, but the consulting firm does not want to release the source code to the company? What would protect the company's interest in terms of the system's upgradability and maintainability?
   A. Registration of the system as intellectual property
   B. Confidentiality agreement
   C. Non-compete agreement
   D. Source code escrow agreement
   E. Access control

2. Which risk goes up the most when an organization outsources systems development?
   A. System integrity
   B. System reliability
   C. System maintainability
   D. Unauthorized data access
   E. System responsiveness

3. Is which systems development phases are flowcharts prepared?
   A. User requirement
   B. Programming
   C. Design
   D. Procedures development
   E. Conversion

4. Which pair of activities can often be carried out concurrently?
   A. Training and procedures writing
   B. Testing and conversion
   C. User requirements development and system design
   D. Project planning and system design
   E. Design and programming

5. When internal auditors are asked by a project manager to provide user requirements to a system development project, they should
   A. refuse in order to maintain independence.
   B. provide as comprehensive requirements as possible by thinking like the business users to ensure the system is complete.
   C. address the system's auditability.
   D. address the system's disaster recovery capability.
   E. facilitate the user requirement workshops.

6. What is the relationship between systems development controls and software change controls?
   A. They are mutually exclusive.
   B. Software change controls depend on systems development controls.
   C. They are inter-dependent.
   D. Systems development controls depend on software change controls.
   E. For a system under development, software change controls should be applied before engaging systems development controls.

7. Which of the following concern is most common to systems development controls and software change controls?
   A. User requirement definition
   B. Testing
   C. Feasibility study
   D. Database design
   E. Emergency fixes

8. What is the correct sequence of system development documentation?
   A. System architecture, user requirements, flowcharts, programs.
   B. Project plan, test plan, user requirements, flowcharts.
   C. Entity relationship diagram, user requirements, Gantt chart, flowcharts
   D. Business case, feasibility study, test plan, user requirements.
   E. User requirements, entity relationship diagrams, system architecture, flowcharts.

9. How do user representatives sign off computer programs?
   A. Review of design documentation
   B. Review of user requirements
   C. Review of computer programs
   D. Testing
   E. Post-implementation review

10. Which phase is avoided when an organization purchases a software package rather than developing it in house?
    A. Defining information requirements
    B. Identifying alternatives
    C. Design
    D. Testing

CHAPTER FIVE – CONTROL AND AUDIT IMPLICATIONS OF EBUSINESS

"The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life." – Bill Gates

In late 1970's, Don MacFarlane, Chief Inspector of the Bank of Nova Scotia, said to his staff frequently that computers were here to grow and grow and we got to keep up. In late 1980's, and audit executive in another large corporation said repeatedly, "technology has its place, its place is not everywhere." Then in mid-1990's, an audit executive in the public sector said that the Internet would drown itself in five years because of overcrowding traffic that would exceed the available bandwidth. I told the public sector audit executive that technology would advance in the next ten years at faster pace than ever before mainly because it had widely reached the consumers. The Internet is everywhere. Large IT companies like Apple are pursuing the Internet of Things (IOT). New applications continue to be rolled out every month. The direction towards a paperless society is not slowing down. For example, it takes a minute to open a bank savings account from home on the Internet and have it ready for use to transfer money from a checking account, right away.

In Chapter Two, we discussed the risk impact of information systems. We concluded that generally, business risks increase proportionally with the use of information systems. This relationship applies to inherent risk, control risk and audit risk. eBusiness involves more IT resources than traditional information systems so we can deduce that eBusiness increases inherent risk, control risk and audit risk.

In addition to discussing the risks of eBusiness, we will cover the legal aspects of information technology (IT). This is because organizations that engage more in eBusiness will find that they have more IT related intellectual property to protect, e.g., eBusiness model, search engine, commercial software and product information. These properties are also more available on the Internet and the risk of copyright infringement is higher. Organizations are more accessible via the Internet so the risk of unauthorized access to trade secret increases.

E-BUSINESS INFRASTRUCTURE

In Chapter One, we discuss the five components of a system: infrastructure, software, procedures, people and information. Of these five components, the one that is most likely to be different between eBusiness and systems that do not use the Internet is infrastructure. Let's see what that entails and what the risks are. Most of the risks are addressed with access controls, which we will discuss in more details in Chapter Eight.

Servers

Customers know of eBusiness by the domain name, e.g., www.united.com. This domain name is attached to a server called a web server. This is the server that takes input from and relay output to customers.

A web server is often the first target of attack, because it is the first server accessed by external parties. It must be configured to withstand stressful traffic and abuse. On the other hand, its configuration should not be as tight as an internal server, otherwise the web server will not fulfill its role of being "opened" to the public. Common configuration parameters include logging as well as ports and services restrictions. A common type of attack on a web server is defacement. Sometimes, instead of defacement, a hacker might change or delete a price, an interest rate or some words in a user agreement. The latter will be less noticeable and the damage can be significant. Organizations should continuously monitor the web server for attacks and changes. A common practice is to frequently refresh the content from an offline version.

The traditional content of a web server consists of data in hypertext markup language (HTML). Increasingly, organizations use eXtensible markup language (XML) to connect links to data and define the nature, format and rules of data, to facilitate eBusiness and particularly business-to-business eBusiness that involves a purchasing organization's system interfacing with a supplier web site directly. For example, an XML link may define that the underlying data table is a table of inventory items where the first field is an alphanumeric product number. Organizations that use XML need to ensure that the links that define data are correct.

A web server usually contains public information and is not used to process financial transactions. A customer transaction is routed to an application server, a server that contains the programs for transaction processing. Before that, when authentication is required, a customer request is directed to an authentication server that contains customer credentials. There is also a database server that contains master and transaction data. All the servers other than the web server should be behind firewalls and more rigorously protected than the web server.

Web Master

This is the person who designs the web site using web authoring software tools. S/he must be well trained, meticulous and have high integrity. The authoring software must be properly configured. Web site design must be thoroughly documented and its content update must be subject to rigorous change control procedures including pre-approval and post verification.

Web Hosting Software

This is the software on a web server that communicates with the browser in a user's computer. In a way, this is the web server's version of a browser. Like a browser, this tool can be configured in a number of ways. The organization should have a standard configuration checklist for the web hosting software to ensure consistency in audit trail and security.

Web Site Tracking Tool

Web sites used to generate revenue would find this tool essential. If misconfigured, the tool may produce inaccurate statistics or fail to capture and analyze traffic. This can result in incorrect charges for advertising. Organizations should periodically review the configuration and verify the statistics produced. This is a highly critical business system for web sites that generate advertising revenue. These sites should have sophisticated web traffic monitoring algorithms to detect click fraud and ensure that advertisers are charged correctly. For example, ten clicks on the same link within a minute should be discarded for calculating advertising charges.

Internet Model

You have probably heard the term TCP/IP in relation to the Internet. Transmission Control Protocol (TCP) is a protocol that is used to deliver data from one network to another and it is important that all organizations including ISPs use this protocol to ensure seamless communication. TCP actually predated the Internet and was used by organizations to connect proprietary networks. Internet Protocol (IP) was added to TCP to form the Internet. IP is used to identify the source and destination by means of the IP addresses. TCP/IP transfer can break a message down to packets increase expedience in transmission. When the packets are reassembled at the destination, the headers are checked to assess completeness of transmission of a message. If incomplete, the receiving router will ask the sending router to resend the packets. TCP/IP structures data in five levels as follows, based on the Open System Interconnection model.

Layer	Main Functions	Hardware	Software	Addresses
5. Application	Lets a user compose data and presents data to the destination	Servers, PCs and smart phones	Web browser and Internet hosting software	Uniform Resource Locator (URL)
4. Transport	1. Breaks a message into packets for expedient transmission via the quickest paths. 2. Assign ports.	Servers, PCs and smart phones	Operating system	Port number
3. Network	Captures the IP address	Servers, PCs, smart phones, routers and switches.	Operating system	IP address and port number
2. Data link	1. Error detection and correction. 2. Captures the media access control (MAC) address.	Servers, PCs, smart phones, routers and switches.	Operating system	IP address, port number and MAC address.
1. Physical	Data transmission	Circuits like phone line, cable, satellite.	Telecommunication software	IP address and port number

Every Internet message is generated at the application layer and lowered successively to the physical layer at which time it is broken into packets. The packets are transmitted on the chosen circuit and when a packet arrives at a destination or intermediate device like a switch or router, it is raised. In the case of a switch (discussed below), the packet is raised to layer 2, a router (discussed below) raises received packets to layer 3. When the packet arrives at a server or user device like a PC, it is raised to layer 5. The only direct communication between devices is at layer 1, the physical layer. That is, each device raises a packet from layer 1 to the appropriate layer desired for the device to manage data.

A simpler form of Internet communication than TCP is Uniform Datagram Protocol (UDP). UDP uses a smaller header and does not check for errors. UDP is used when speed is more critical. It is therefore more often used for video and audio streaming, this is why such streaming sometimes has low quality and precision compared to financial

data. Secondly UDP is also used by a router to find a computer and direct content to the computer. If the computer cannot be found, the router will send a second request and a third request etc. until the set timeout period expires for that message.

Internet Addressing

There are four types of address:

- uniform resource locator (URL) at the application layer
- Internet Protocol (IP) address at the network layer
- media access control (MAC) address at the data link layer
- port at the transport layer

Every Internet transaction has to include these addresses. A URL is essentially a web site address like www.ontario.ca. An IP address is a numeric address consisting of four 8-bit bytes and in more advanced networks, four 32-bit bytes. A MAC address is hard coded address assigned to a network adaptor by the manufacturer, like a vehicle identification number. URLs and IP addresses can be assigned dynamically. In other words, a computer may be assigned different URLs or different IP addresses from time to time, however, the MAC address usually does not change. It is specific to a network adaptor installed in a computer or device like a smart phone. For a smart phone, the MAC address stays with the phone regardless of the SIM card. The MAC address is therefore crucial for a network to route traffic. It also provides a permanent audit trail of which computer was used to carry out an activity and this information is useful in establishing an audit trail and forensic investigations.

There are sometimes, not by intent, duplicate MAC addresses between manufacturers, especially caused by small vendors. Thus, it is important for a user organization to record and scan MAC addresses periodically to detect duplicates. MAC addresses can also be spoofed, i.e., changed by a rogue user using special tools, to hide identity. An organization can prevent it by locking MAC addresses specific physical ports on the network switch. This method is not fool proof, it at least reduces the scope of spoofing, i.e., restricting spoofing to within the devices connected the particular switch. This is why it is also important to periodically validate MAC addresses by tracking the assignment of IP addresses to MAC addresses and physically verifying MAC addresses.

Traffic on the Internet is generally routed using IP addresses. Every device on the network is assigned such an address. Organizations should subscribe to enough IP addresses for its users and servers. A device needs an IP address only when it is connected to the network. Workstations and laptops can be assigned temporary IP addresses. Servers should have permanent addresses in order to lessen change to the domain name servers, which we will discuss below. Organizations should try to hide its real IP addresses from the public to prevent attacks by using network address translation methods, i.e., translating an internal IP address to an external IP address and vice versa. IP addresses around the world are assigned, for a fee, by Internet Assigned Numbers Authority (IANA), a not-for-profit organization in the United States owned by Internet

Corporation for Assigned Names and Numbers (ICANN), also a not-for-profit corporation in the United States. ICANN controls domain names to avoid duplication and keeps track of what organizations own what domains.

IP addresses are geographically assigned, i.e., there are ranges for Africa, Asia Pacific, Europe, North America and Latin America. Within each of these ranges, addresses are assigned by country and then grouped by region within a country. It is therefore easy to tell where an IP address is assigned to.

Most IP addresses are composed of four 8-bit bytes. When expressed decimally, an IP address can theoretically range from 000.000.000.000 to 255.255.255.255. For example, IP address 192.168.0.107 is assigned by my Internet service provider (ISP) to my computer right now at 10:46 pm on February 21, 2014.

The current 8-bit scheme, using IP Version 4, can accommodate 4,294,967,296 addresses and is not enough. Many organizations dynamically ration IP addresses hence limiting their networks. A new range, called IP Version 6, has been introduced to use four 32-bit bytes for each IP address. This can accommodate 340 undecillion addresses, or 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses, and that means roughly 47,135,955,035,839,400,000,000,000,000 per person. Countries are asking for their blocks of this new range. For example, China has requested 32 billion addresses. Some large organizations and ISPs are adopting IP V6, which is not interoperable with IP V4. There is no IP V5.

A port is a conventional "door" or mailbox used on the Internet to standardize the types of Internet data traffic. Common ports include port 80, which is used for web browsing, port 443, used for encrypted Internet traffic like eBusiness, and port 25, which is used for traditional email (not browser email) based on the simple mail transfer protocol, e.g., email via Microsoft Outlook. There are thousands of ports recognizable on the Internet. An organization can configure its systems to use any port internally for tailored applications.

Domain Name Server

This is a server that is used only in an IP environment. It translates URLs to IP addresses. A URL may be a domain name or an extension thereof (part of a domain), e.g., www.ontario.ca or www.cica.ca/itac. For the Internet to be universally operable, every URL is assigned an IP address.

A DNS uses a table to translate each URL to an IP address and vice versa. The "vice versa" occurs usually for research and investigate purpose. For example, if a network administrator finds that an IP address is causing an enormous amount of traffic load, s/he can look up the URL that uses the IP address and contact the system administrator. The table is supplied by ICANN and updated frequently. Large ISPs have very up-to-date tables.

A DNS also contains internal references for IP address translation in order to route traffic within an intranet and also to route traffic received from an ISP to internal servers and workstations. Small organizations may not have DNS and may instead rely on the ISP. For those with DNS, the tables may be less up to date and any URL that cannot be translated to an IP address is deferred to the ISP for translation.

A DNS is a common target of hacking. If a DNS is down, traffic that needs the DNS for IP address resolution (translation) will be stopped. Worse, if the DNS table is changed by a rouge person, e.g., substituting a bank's IP address with that of a hacker site, a bank customer can be directed to the hacker site.

Organizations should have redundant DNS and place their DNS behind firewalls. Changes should be monitored. Periodic test of IP resolution should be performed. A DNS can be used by an organization to prevent employees from going to undesirable sites by routing those URLs to a static server that returns a warning message.

Some DNS are placed at the network perimeter mainly to find the IP addresses of deep URLs. A deep URL is one with suffices to the domain name, e.g., http://www.yorku.ca/yorkweb/cs.htm. If I key this in from a browser at home, my ISP may be able to resolve it to an IP address in York University. However, my ISP may not know which server hosts the document I am looking for. If York University has a DNS at the network perimeter, it can then take me to the appropriate server.

Firewall

An organization that hosts a web site should have at least one firewall. It is better to have multiple firewalls. A firewall screens incoming traffic to determine what is admissible, e.g., by IP address or port. It can also prevent certain outgoing traffic. We will discuss firewalls in detail in Chapter Eight.

Router

A router is a device that connects two networks or network segments. Many of us have simple routers at home that connect the Internet modem to different devices like computers, printers and voice-over-IP boxes.

Data travels on networks in packets. A packet is a fixed group of bytes to facilitate efficient use of network transmission resources. For example, a long transaction or message may take longer to be transmitted if the network circuits are very busy. By segmenting every message or transaction to packets with fixed length, a message or transaction can be transmitted via different circuits and regrouped at the destination, hence increasing efficiency. A typical packet has 1,024 bytes.

For packets to be reassembled at the destination, each packet must have control information, which is recorded on the packet header. Critical header information includes:

- source IP address
- destination IP address
- port number
- packet size
- ID and sequence number of the packet within the message to allow the destination network point to reassemble the packets

The header information is then followed by the actual data, e.g., "Gerald Chan to be Supreme Court justice".

The type of service can be used by the network to prioritize traffic based on the port number, e.g., web surfing takes precedence over email. This is only practical internally as an organization cannot dictate how the ISP prioritizes traffic.

The more packets are used in a message, the more overhead is incurred and the slower the traffic is. However, the offset is that a small number of packets means each packet is longer and the chance of finding space on the Internet to deliver a long packet is lower and that means it takes longer to deliver. The optimal packet size depends on the length of messages. If there are a lot of short messages, it does not make sense to use a large packet size. A network can be configured to vary the packet size based on type of service or time of day.

A router plays a large role in determining which circuit a packet will travel on. It is, in a large sense, a traffic controller and director. Because it directs traffic, it can be used as a perimeter firewall. A router has its own operating system similar to a computer's operating system but less complicated. It has configuration parameters that can affect efficiency, audit trail and security. If a router is down, network traffic can come to a standstill. It is therefore important to have redundant routers.

A router uses simple network management protocol (SNMP) community strings to authenticate workstations and servers. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (router) and the SNMP agent (a PC or server). The community string is included in every packet that is transmitted between the SNMP management station (router) and the SNMP agent. Organizations should use complicated SNMP strings, just as it is important to use complicated passwords.

Switch

A switch is similar to a router but less configurable. It generally works at layer 2 and uses the MAC address to filter and forward traffic. Because most devices' MAC addresses are not broadcast externally, a switch tends to be used in internal networks. One exception is smart phone email traffic where the MAC addresses can be included and a switch can then be used to filter and forward such traffic. A switch is faster but has less audit trail than a router. It is not recommended to replace a router for forwarding business transactions. A switch that connects with external network nodes operates at layer 3. A

node is a network access point. A switch also uses SNMP community strings. A key difference between a switch and router is that a router can perform much more logging than a switch.

Internet and eBusiness Service Providers

An ISP is increasingly becoming as important to an organization as the utility company or telephone company. In fact, many organizations use their telephone companies as ISPs and some utility companies lease their fiber infrastructure to ISPs. An ISP's outage because of a virus attack or router problem can cripple eBusiness for an organization. It is important for user organizations to select reputable ISPs and include availability commitment and responsibility for outage in the contracts.

In addition to using ISPs, some organizations use eBusiness application service providers. An example of such a provider is J. P. Morgan's Order to Pay service that processes orders and payments. Another type of eBusiness service is a content delivery service that stores an organization's data close to customers to improve user friendliness and reduce bandwidth cost. Akamai, for example, operates almost 10,000 Web servers located near the busiest Internet network access points. These servers contain the the most commonly requested Web information for some of the busiest sites like Certified General Accountants Association of Canada, Yahoo!, Monster and Ticketmaster. This approach is called edge computing, i.e., placing information on the edge of an organization's sphere of influence to make it easily accessible to customers. Edge computing increases the risk of information dispersal and data inconsistency. User organizations should have tight contracts with network service providers with respect to due diligence over information maintenance and access controls to prevent unauthorized change.

A somewhat similar computing approach involving service providers is cloud computing, whereby an organization stores information in an ISP's server to interact with information in local servers throughout the day to expedite transaction processing and reduce cost. Cloud computing increases the risk of unauthorized access because more devices are interfaced. User organizations should ensure that their contracts with the ISPs provide for adequacy security. User organizations also have to review their firewalls, intrusion detection system and intrusion prevention system in light of the increased risk of cloud computing. We will talk about these access controls in Chapter Eight. The following is a recent incident that demonstrates the risk of cloud computing.

The dangers of using consumer cloud storage systems became clearer earlier this month, when a hacker claimed that he accessed presidential candidate Mitt Romney's Dropbox storage and email accounts using an easily cracked password. The apparent hack of Romney's accounts came on the heels of IBM's rollout of a bring-your-own-device (BYOD) policy that bans the use of Dropbox due to concerns that hackers could easily access sensitive information stored there. Such examples make it clear that it's risky to keep corporate data on consumer-oriented cloud storage systems, say IT executives and analysts. "IBM has the world's biggest BYOD program, and they just locked down Evernote and Dropbox because they discovered their future product plans and all sorts of really sensitive data was being beamed automatically out to these services," said Dion

Hinchcliffe, an executive vice president at IT consulting firm Dachis Group. Though companies are increasingly tightening their BYOD policies, most have yet to address the use of consumer apps and services such as cloud storage on mobile devices.

Source:
http://www.computerworld.com/s/article/9228147/BYOD_exposes_the_perils_of_cloud_storage?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+computerworld%2Fs%2Ffeed%2Ftopic%2F17+%28Computerworld+Security+News%29; May 30, 2014.

RISKS OF E-BUSINESS

In Chapter Two, we examined the risks of IT and concluded that inherent risk, control risk and audit risk increase with the growing use of IT. eBusiness uses more IT compared to the conventional business model. Therefore, risks increase when eBusiness is used. Let's review the six risk criteria of incompleteness, unauthorized, inaccuracy, untimeliness, non-occurrence and inefficiency and see how they are affected by eBusiness.

Incomplete Transaction

eBusiness transactions are recorded at the point of sale, so the risk of a transaction not getting recorded is generally lower than that for a paper based transaction. However, because customers perform data entry, the risk of incomplete data is higher than that of a transaction entered by a customer service representative. There is also the concern that even though recording is instantaneous, the human action required, such as to arrange for shipment, may not be carried out because of some information falling through the crack. Overall, the risk of incomplete processing can be rated as moderate.

Unauthorized Transaction

The main concern about eBusiness is security. This translates to the risk of unauthorized transactions. It is widely recognized that this risk is higher than that in a non-Internet business environment.

Inaccurate Transactions

In eBusiness, customers perform the data entry. This affects accuracy because many customers are not good typists and they tend to be in a rush. The risk of inaccurate transactions is therefore high. Also, eBusiness transactions are more subject to hacking to change transactions for the benefit of the hacker or just to distort processing. For

example, a hacker can change the interest rate table displayed to mislead customers. Another example is to change a transaction string while a transaction is in progress. The second example is described in more detail here.

Here is a hypothetical example of a web string built up by web server as a customer carries an online transaction:
www.chanman.com/orders/final&custID=112&num=55A&qty=20&price=10&shipping=5&total=205

This string shows that customer #112 is buying 20 units of product 55A at $10 each and the shipping charge is $5, yielding a sales amount to be charged to the credit card as $205 before sale tax. So far so good.

A hacker who gains unauthorized access to this string can edit it as

www.chanman.com/orders/final&custID=112&num=55A&qty=20&price=10&shipping=5&total=25

Now, the amount charged before tax is $25 and Chanman company is losing $200.

The web string is used to display the progress and result of a transaction to the customer and then ask the customer to confirm before giving out the credit card number. If an organization simply takes the result of this web string to charge the credit card, a string that has been altered by a hacker will lead to incorrect revenue. To mitigate this risk, organizations should recalculate the invoice amount behind the web interface before finalizing the transactions. Such recalculation is made by the application and it takes place in the application server.

Untimely Transactions

Customers buy on the Internet for convenience. Internet transactions are processed immediately and the risk of untimeliness is therefore lower than the conventional transaction model. The risk of untimely processing is low.

Non-occurrence

Because of open access and the lack of paper trail, the risk of a recorded transaction not representing an actual business event is higher when eBusiness is used. The concern often extends beyond the transaction, to also the parties. Is the customer or the supplier real? We would therefore consider the risk of non-occurrence, i.e., information in the system not reflecting real transactions, to be higher than that for conventional transactions.

E-BUSINESS CONTROLS

When an organization offers eBusiness, it should review the current general and application controls in relation to the increased risks. Usually, the following internal controls have to be expanded or added. These controls are in addition to the existing application controls in transaction processing systems because in most cases, eBusiness is a new or additional way of conducting business but the transaction processing should not differ significantly whether the order is placed online or in person. We discuss these controls in various chapters.

- Boundary checking – Chapter 8
- Digital certificate – Chapter 8
- Digital signature – Chapter 8
- Disaster recovery plan – Chapter 3
- Edit checks – Chapter 6
- Encryption – Chapter 8
- Firewall – Chapter 8
- Intrusion detection system – Chapter 8
- Intrusion prevention system – Chapter 8
- Online backup – Chapter 3
- Recalculate transaction amount behind the web server to nullify change made by a hacker – Described above
- Redundant communication lines – Chapter 3
- Redundant servers – Chapter 3
- Web site refresh – Chapter 5

ELECTRONIC DATA INTERCHANGE

Electronic data interchange (EDI) predated the Internet. The Internet, however, has made EDI more affordable and widespread. EDI is a protocol that allows two organizations to exchange accounting documents like purchase orders and invoices without human intervention. Company A can send batches of purchase orders to companies B, C, D etc. Company A can also send invoices to companies X, Y, Z etc. Each of these companies can send purchase orders, invoices and other common transaction documents electronically so that the documents can be imported to the accounting systems of the recipient companies. This saves paper, postage and key entry. With lower transaction processing cost, companies can order more frequently and therefore keep less inventory. This means there are less average inventory and accounts payable, which also means a smaller balance sheet. Yes but, if less money is tied up in inventory, there is more cash, so why is the balance sheet smaller? Companies that use EDI are progressive and they don't keep much idle cash. They will use the cash to expand, so the balance sheet is relatively smaller in relation to the income statement than organizations that do not use EDI. As an EDI organization expands by for example, opening more stores, its balance sheet will grow again; at least, in the short term, the balance sheet is smaller in terms of

inventory accounts payable, not in terms of net assets. This lessens substantive audit work. Less substantive testing does not mean the audit is easier; the auditors have more internal controls, EDI controls, to test.

EDI can also be used for payments. Paying organizations send remittance advices to their banks. Their banks then distribute the remittance advices and funds to the banks of the payee organizations. The payees' banks in turn send the remittance advices to the payees and credit the payees' accounts. This avoids the risk of check bouncing.

In order for organizations to exchange transaction documents and have their systems interpret the documents, the format must be standardized. There are two common EDI transaction formats, American National Standards Institute (ANSI) for the United States and Canada, and EDI Standard for Finance, Administration, Commerce & Transportation (EDIFACT) for the rest of the world. Each organization using EDI needs a translation software tool to convert its own transaction system format to the common format and vice versa. The translation software can be developed in house or purchased from EDI software vendors. When installing the translation software, an organization will import its local data formats for the software to learn. Once imported, every time outgoing transactions are loaded to the EDI server, the software will convert the documents to the standard format. Also every time incoming transactions are received into the EDI server, the translation software will convert the standard format to the organization's own format.

The attractiveness of EDI is somewhat reduced by an increasingly sophisticated use of XML for web sites. If company A can automate its purchasing system to place orders on the web site of company B which is highly XML driven, company A may decide not to submit orders using EDI. Another trend in EDI is that two organizations that have a close business relationship may opt to use XML as the data standardization method instead of adopting ANSI or EDIFACT.

ANSI and EDIFACT accommodate a long list of business documents, categorised as follows:

- Air and motor
- Automotive transportation
- Delivery
- Engineering management and contract
- Financial
- Government
- Health services
- Insurance
- Manufacturing
- Material services
- Mortgage
- Ocean transportation
- Payments
- Purchase order
- Product services
- Quality and safety

- Rail
- Tax services
- Warehousing

EDI transmitted documents are fed to the recipient's transaction systems directly, there is no need for data entry. Hence the risk of incorrect data entry is reduced in the recipient organization.

Risks of EDI

The risks of EDI include incomplete transmission, unauthorized transmission, inaccurate transmission (e.g., to the wrong parties), untimely transmission, transmitting documents that do not reflect real business transactions (non-occurrence) and inefficient transmission. These risks all relate to transmission because EDI is a transmission protocol. Transactions are already prepared before they reach the EDI server so the risks of inaccuracy and unauthorized transaction generation etc. are less relevant.

Incomplete Transmission

This risk is significant because of the large volume of documents. If the volume is small, an organization will likely not want to incur the overhead of EDI. Organizations should apply batch total verification and require acknowledgement from the recipient parties to confirm completeness. A batch total is a total of a transaction batch taken at one point, and at a later stage when the batch is further processed or transmitted, another total is taken, the two totals are then compared to ensure completeness of processing or transmission.

Unauthorized Transmission

This can occur if the person invoking the transmission is not authorized or the batch job for scheduled transmission was set up without authorization. The impact is significant because one unauthorized click can send a lot of documents. The controls over this include mainly access control lists, passwords and management review of the transaction log.

Inaccurate Transmission

This risk is relatively low because EDI is used to transmit documents instead of generating the transactions. The preparation of a purchase order or invoice is independent of EDI, or in other words, the data going on a purchase order or invoice is not affected by the use of EDI.

The inaccuracy risk with EDI mainly has to do with translation to and from the ANSI or EDIFACT EDI format and maintaining the list of transmission destinations. The control would be to periodically test the translation software and validate the transmission destinations. Reconciling the transmission log totals to the application systems would also detect inaccurate transmission.

Untimely Transmission

The risk is quite low because EDI is much faster than using Canada Post or couriers. Timeliness would be impaired if the transmission schedule is incorrectly changed or set up. It could also occur if the person responsible for invoking the transfer forgets or is sick and there is no backup staff. To mitigate these risks, management should periodically review the transmission schedule and implement an incident response plan.

Transmitted Documents not Representing Real Transactions

This risk is moderate because EDI is used only for transmission, assuming there are strong controls in the application systems to mitigate the risk of non-existence. The risk is not low because of the powerful access capability of the person who invokes an EDI batch. If the transmission is automatically scheduled without human intervention, the risk of non-occurrence is low. In addition, management should implement access controls over the generated EDI files to prevent manual insertion.

Inefficient Transmission

Organizations adopt EDI for efficiency gain because there is savings in key entry, postage, paper and inventory level. To ensure the intended savings is achieved, organizations should minimize delay and check the accuracy of format translation. They should also monitor the transmission log and counter party acknowledgement to detect and address transmission delay.

EDI Controls

EDI is a transmission protocol so the internal controls should address data transmission. The transaction processing controls substantially do not change. Some of the transaction processing controls will change in form. For example, edit checks will be performed on transaction data when the transactions are read by the recipient organization's system instead of when data is entered by people. The following are the basic EDI controls that address data transmission.

- Acknowledgement of transfer completeness
- Access control lists to restrict who can initiate EDI transfers
- Batch totals of transfers and reconciliation of batch totals (batch totals will be discussed in more detail in Chapter Six.)
- Digital signature to assure the trading partner that the data transfer is authentic.
- EDI contracts with trading partners
- Encryption to protect transmitted data from being viewed by unauthorized parties.
- Transfer log and its review

The EDI contracts should describe the following:

- Digital signatures if any.
- EDI transmission standard and protocol, e.g., ANSI, XML, email transmission, browser based transmission, file transfer protocol (one organization sending files to another organization without using email or a browser, an inherently less secure approach with less audit trail).
- ISPs
- Legal credibility of transactions.
- Place and time of acknowledgement.
- Place and time of message receipt.

Some of the above are access controls, which we will discuss in Chapter Eight.

MOBILE EBUSINESS

Mobile devices are increasingly used in business transactions. Common examples are smart phones, laptops and radio frequency IDs (RFID). The risk implications are mainly related to security which will be covered in Chapter Eight. However, for RFID, the risks go beyond security and include the validity, completeness and accuracy of asset tagging.

Radio Frequency Identification

RFID is increasingly used in business and governments to track the whereabouts of equipment and inventory. Common applications include consumer products, toll roads, libraries and even hospital supplies. The benefit of technology application depends on the correctness and robustness of configuration as well as the reliability of the supporting and interfacing systems. This principle, of course, also applies to RFID.

Technical Aspects of RFID

Unlike bar code scanning, RFID does not require line of sight in order to be read. This makes its application more diversified and flexible. RFID technology basically comprises three components. These components include a tag, a reader and the system that records the information transferred by a reader. A tag, which can also be called a transponder, is a

small device that is made up of an antenna and a microchip. The tag transmits frequencies to a reader which verifies and analyzes the information being transmitted. The reader then transfers the information to a server for further analysis and storage. An example of RFID applications is toll road usage tracking. The following diagram illustrates the data flow in an RFID application.

Source: Singapore Government web site

RFID Tags

A tag or transponder can be passive or active. An active tag has a battery that sends power to the microchip and allows the chip to send information to the reader. It can be tracked on an RFID network. A passive tag, which is less expensive, usually does not have a battery but it receives power from a nearby reader. Active tags generally have the capability to receive "read" and "write" commands. In other words, they can receive information to be stored, in addition to their ID numbers, and transmit information to a reader. A passive tag can only transmit information. Some passive tags have their own batteries because the readers are too far like toll road metering. RFID chips are generally too expensive to be equipped on small items like a can of Coke as it costs about 10 cents each. However, it can be attached to a pallet of Coke.

Common Applications

RFID is increasingly used as an inventory control measure. By outfitting each product or case with a tag, a company can track the quantity and location. Some large retail chains like Walmart require suppliers to outfit their products with RFID tags. Hospitals can use RFID to track supplies, inventory level, bed vacancy and patient status (e.g., check-in and check-out). Tags can also be given to nurses, doctors and other workers to act as access keys.

RFID is also increasingly used as transit tokens. For example, Hong Kong's Octopus system issues RFIDs in the form of a plastic card. This card can be used for public transit, convenience store purchases, registered office and condominium building access, and person-to-person money transfer. The value of the card can be reloaded in almost all convenience stores at denomination amounts of $50, $100, $150 etc. Credit cards and the Octopus card are equipped with RFIDs that can be tapped on a merchant's reader for small purchases to be processed using a technology called near field communication (NFC). Two smart phones can be tapped on each other to exchange information. Smart phones have NFC so the phones can be used as credit cards for small purchases. NFC has shorter range than Bluetooth, up to 20 cm. With NFC capability, phones and credit cards warrant more safeguarding. The "tap to send" and "wave to pay" features can be disabled by the phone owner. The manufacturer of each card or phone can shorten the distance; e.g., a credit card has to be tapped on the terminal for payment to be registered. Most retail outlets accept this method for purchases up to $100 each.

NFC cards are also used widely for access to office and apartment buildings. In Hong Kong, a resident can use the same Octopus card for transit, small purchases, taxi rides, home access and office access. The merchants, office building management and apartment building office just have to subscribe to this access service through the "Octopus" company.

Joseph Krull doesn't have a chip on his shoulder. But he has one in it. The San Antonio security consultant is one of a small but growing number of people who essentially turn themselves into wireless network nodes for the sake of making personal information available to authorized parties with the wave of an RFID scanner.

In Krull's case, the chip was implanted two months ago so hospital staff could access his medical information quickly in emergency situations. Others are "getting chipped," as those in the know call it, for everything from entertainment to personal safety. Krull's chip is basically the same kind of RFID-based technology that's been used for years to tag dogs so they can be identified if lost, except the human chip works on a different radio frequency.

"I have a blown pupil, a detached retina, in my left eye from a skiing accident," says Krull, explaining his decision to have a physician with a syringe stick a chip in him under local anesthetic in what he described as a fairly simple procedure. "I'm supposed to wear a MedAlert bracelet because one of the indicators of a head injury is a blown pupil. One thing they might do in that kind of emergency is drill holes in your skull." The thought of having holes unnecessarily drilled into his head, because of a misdiagnosis during a medical emergency, got Krull thinking about having a chip implanted after he heard about it during a conference in Spain. "I wanted to get chipped," he says. Krull can access his personal data stored online at VeriChip's portal and make any changes he wants by using a reader and a PIN code. Krull elected to store his medical information and address, phone numbers, fax and e-mail at the Web site. One catch with RFID

implants is that emergency technicians won't necessarily know that a patient has a chip under his or her skin. But VeriChip is giving away its RFID scanners to hospitals in the hope of building momentum for use of chips.

Fellow implantees include the attorney general of Mexico City and some of his staff, who were chipped to help identify them in the event that they become crime victims. Some are getting implants just for kicks - a nightclub in Glasgow, Scotland, called Bar Soba, offers to implant chips in its guests so the bar can prepare each patron's favorite drink the minute he walks in. Also getting a chip shot was John Halamka, the CIO at Beth Israel Deaconess Medical Center in Boston and Harvard Medical School and a practicing physician. Halamka got chipped last December in an experiment of his own making. The outspoken CIO says he's had "no side effects, no pain, no change in muscle function and no migration of the chip" in the months it's been in him, despite rock and ice climbing where Halamka exposed himself to "extremes of temperature, wind, water."

Halamka decided to be a chip guinea pig as the result of experiences he had while working in emergency medicine at Harbor-UCLA Medical Center in Carson, Calif. Emergency care often put him in the situation of having to identify patients who were without ID documents and unconscious, non-verbal or mentally ill. That often involved picking out clues found in their belongings such as a clothing label. "I would inevitably reunite the patients with their loved ones, but not before significant worry and possibly unwanted medical interventions had occurred," Halamka says.

In his CIO role Halamka is responsible for all clinical, financial, educational and research technologies for 3,000 doctors, 12,000 employees and 2 million patients. After the FDA approved the implantable chip, "I felt I was in a unique position to pilot the technology," Halamka says. "That means that when a scanner is passed within 6 inches of my arm, my medical identifier is displayed and can be used by authorized healthcare workers to retrieve information about my identity and medical history via a secure Web site."

Halamka emphasized his role at present was not that of chip advocate for hospitals but as a real-life test case. Though he said that Alzheimer's patients might benefit from RFID chips one day, as long as it's clear the patients gave informed consent to have a chip implanted. The chip is expected to last at least 10 years based on pet experience. Halamka says it's safe for MRI scans, and he sees no evidence the chip can be deactivated through magnetic energy. "I have flown to several dozen cities since the implant and have not triggered any airline security systems," he notes. The chip is not a GPS.

However, Halamka said there were privacy concerns that should be addressed. He pointed out that an RFID scanner theoretically could record his presence while he was making a purchase, and on a repeat visit it would be possible to identify him and his previous purchases using that information for marketing purposes.

"Spam, generated by the presence of your body, is theoretically possible," he says. He says there's no legislation to preclude RFID scanning of an individual for anonymous tracking, which could be "analogous to the spyware and adware infecting our computers after surfing Internet sites." The potential for hacker abuse shouldn't be underestimated, he adds.

The security issue "must be understood as one of the risks of having an implanted identifier," Halamka said. Nonetheless, he has listed his identifier as part of his medical record in the Beth Israel Deaconess medical record system, called CareWeb, so that a physician, with his consent, could enter the RFID tag information to retrieve his medical history.

"I have no regrets," Halamka says about the whole implant experience, even though removing the chip would require minor surgery. And he would consider upgrading himself with a new chip, too, should a better one come along.

Source: Network World, April 4, 2005

Risks Associated with RFID technology

One fairly wide concern about RFID is privacy. For example, if an organization attaches a tag to a consumer product, can the organization track where the product is used and perhaps who uses it? The risk and control implications of RFID, however, go beyond privacy. In fact, the basic reliability factors of completeness, accuracy, authorization, timeliness, occurrence and efficiency have to be considered as they can be compromised by inadequately controlled deployment of RFID. Here are some specific risks in using RFID.

Privacy Breach

This often arises as organizations are increasingly empowered by technology to collect, store and analyze personal information or to analyze and infer customer purchasing pattern. This can lead to violation of privacy legislations and perceived lack of control over safeguarding customer personal information. As a result, the use of RFID may be resisted.

Given that RFID tags are so small and not noticeable, people are at risk of having tags sewn into clothing and being scanned unknowingly. Tags can also be placed in automobiles and other personal belongings and people can once again have their movements or actions tracked. The reason this is a major privacy risk and concern is that each tag usually is assigned a unique bar code. This can lead to the issue of identity theft. With so much information being passed through these small tags, the likelihood of interruption and corruption is high. As a result, identity theft is a larger concern now that RFID is increasingly used.

An issue that is already being discussed is the implementation of RFID tags in employee ID cards. While organizations claim it is for operational purposes, it essentially allows the employer to monitor every movement that the employee makes. Further, in some cases, the tags are implemented without the knowledge of the employee. It is a pressing issue that begs the question: What is acceptable and what is not? Organizations should ensure they comply with the relevant privacy regulation and communicate to employees that monitoring of business activities will be conducted without violating the relevant privacy regulations. Overall, RFID technology poses security and privacy threats. If the technology falls into the wrong hands it can be used to track personal information and whereabouts. Given that the technology only needs a tag to be scanned for something to trigger, terrorist attacks could be conducted more easily. Also, visitors or unauthorized employees can place readers to sniff information being transmitted.

Tracking or Interception by Hackers

Hackers and criminals can track the radio frequency and alter data being transferred. They can also intrude servers and change the table that correlates tags to assets or people. Reader configuration can be changed to redirect traffic or have their logs compromised.

Unauthorized Tag Removal

As a result, inventory movement cannot be tracked and asset will be overstated in the financial statements. Incorrect inventory positions can lead to inability to meet customer demands. Tags assigned to medical equipment or patients, if removed without authorization, can cause health hazards.

Incorrect Description of Asset Information in an RFID

If the information being tracked is incorrectly recorded in an RFID, it can lead to asset misstatement, the inability to satisfy customer demands or unnecessary funds tied up in inventory etc. For example, the RFID attached to a pallet of Coca Cola Classic may be the RFID intended for Coca Cola Zero. Alternatively, instead of putting on the wrong

RFID, the encoding of product information on an RFID may be incorrect, e.g., recording on the wrong product number for Coca Cola Zero, an invalid number that is not consistent with the product catalog sent out by Coca Cola to retail stores.

Tag Failure

A tag may fail because of faulty manufacturing, damage by environmental factors, incorrect installation or an expired battery. If this is not monitored, information tracking will be incomplete. The large number of RFIDs in most applications can make this risk significant.

Incorrect Expiry Dates

Tags that are attached to access passes, passports and perishable items must have expiry dates. If the date is incorrect, assets can be lost, hazardous food may be sold, or inappropriate access may be granted.

Failure to Attach Tags on Assets Being Tracked

An organization may fail to attach a tag on certain units that are intended to be tracked. This risk increases as the population of the units grows and manual effort is involved. The result will include understated inventory, incomplete information about individuals or denial of legitimate access.

Incomplete or Incorrect Data Transmission

This can occur because of faulty tags, reader malfunctions or communication line breakdown. Information stored on servers will therefore be incomplete or inaccurate. Updates from servers to active tags may also be lost resulting in inconsistent or inaccurate tracking.

RFID Controls

To mitigate the above risks, management should consider adopting the following control practices.

1. Review the RFID application project plans and system functions with the chief privacy officer to ensure compliance with privacy regulations.

2. Subject RFID systems and devices to rigorous integration and user acceptance testing.

3. Periodically perform network penetration testing to assess the exposure to hacker and worm attacks.

4. Perform regular physical check of devices.

5. Perform regular testing of data capture and tracking to ensure accuracy.

6. Frequently validate the inventory of activated RFID devices.

7. Regularly review reports of activation and deactivation to ensure tag movements are authorized.

8. Regularly review statistics about tag data transfer volume and delays.

9. Ensure servers have adequate intrusion detection and virus detection software.

10. Deploy network transmission integrity checking techniques like redundant data check.

11. Educate customers and employees about privacy risk and measures to protect their privacy when using RFID, e.g., removing RFID tag when a suit is sold and not carrying unused RFIDs around.

12. Perform cyclical and year end inventory count instead of relying only on the inventory information on RFID tags.

Financial Considerations in Using RFID

It is not hard for management to be sold on the benefits of RFID. The costs must also be comprehensively considered. They include the following:

- Tags
- Readers
- Servers
- Software

- Conversion from existing data
- Training
- Preventive maintenance
- Systems development and maintenance

In the rest of this chapter, we will discuss the legal issues that have either arisen or been accentuated with eBusiness, including privacy.

ELECTRONIC COMMERCE ACT

Many jurisdictions in developed countries have legislations to protect consumers in eBusiness transactions. Ontario's Electronic Commerce Act defines the legal enforceability of e-commerce transactions. This Act aims to reduce the legal uncertainty associated with electronic communications and contracting. Some other provinces have similar legislations.

There are three main points. First, the Act recognizes an electronic signature as legally binding. Secondly, the Act recognizes the interaction between electronic agents or between an electronic agent and a person as legally binding in constituting an offer or an acceptance. Thirdly, and most important to auditors, is that the Act puts the onus on merchants to put in place reasonable measures to prevent errors, that includes internal control.

Electronic Signature

The Act defines electronic signature as electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document." This is construed to mean more than a scan image of a handwritten signature. It basically means digital signature, composed using cryptography. We will discuss digital signature in Chapter Eight.

Offer and Acceptance

Offer or acceptance can take the form of interaction between an electronic agent and an individual or between two electronic agents. The Act defines an electronic agent as "a computer program or any other electronic means used to initiate an act or to respond to electronic documents or acts, in whole or in part, without review by an individual." This increases the importance of systems development and software change controls.

Errors Prevention

The Act says:

An electronic document made by a natural person with the electronic agent of another person has no legal effect and is not enforceable if the natural person made a material error in the document and

(a) the electronic agent did not provide the natural person with an opportunity to prevent or correct the error;

(b) the natural person notifies the other person of the error as soon as practicable after the natural person learns of the error and indicates that he or she made an error in the electronic document;

(c) the natural person takes reasonable steps, including steps that conform to the other person's instructions to return the consideration received, if any, as a result of the error or, if instructed to do so, to destroy the consideration; and

(d) the natural person has not used or received any material benefit or value from the consideration, if any, received from the other person.

This section puts the onus on eBusiness merchants to put in place reasonably preventive controls, e.g., placing a limit on the number of books ordered per title, or alerting a securities trading customer that the number of shares of a common stock s/he wants to buy is the same as his or her current holding (in case the customer means to sell). We will discuss these controls in more details in the next chapter.

PRIVACY

Many people refrain from using eBusiness because of their concern about privacy. The general public has never been more concerned about information privacy. The concern has been heightened in recent years by technology advances, identity theft and security breaches. The exponential increase in computing power allows organizations to store more and do more analysis of personal information, potentially breaching privacy.

Hackers are now more entrepreneurial. They are less interested in defacing a web site or sending a worm to bring down a web site without financial gain and running the risk of going to jail. They are more interested in stealing identity and selling to criminals.

Before we go further, let's be clear on what information privacy means. It means the confidentiality of personal information, not business information, although personal information can have business implication. For example, privacy does not apply to a company's business strategy. Privacy also does not apply to someone's telephone number if the number is listed, because it is no longer confidential. What is personal information in the context of privacy legislation? It is confidential information about a person collected from the person. The "personal" nature of information has to be interpreted in the context of where is it held and used. For example, my salary is not personal information when it is stored in the systems of my employer; this is because I did not

provide my salary to the employer, my salary is set by the organization that employs me. However, my salary which I have given to my bank for a credit application is personal information in the bank. How confidential does information has to be in ordered to be covered by privacy legislations. Courts and governments have construed that to mean information about a person provided by the person which a reasonable person in that circumstance would consider it important to be kept private.

Laws and regulations in most developed countries define the following to be sensitive personal information:

- Date of birth
- Personal ID number like a social security or social insurance number
- Consumer purchase history
- Finance
- Medical or health condition
- Offence or criminal conviction
- Sexual preference
- Trade union membership

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to all businesses and other organizations where there is no provincial privacy legislation for the private sector. The private sector includes all businesses and organizations, whether for profit, that are not governments or organizations substantially funded by a government. Corporations whose shares are wholly owned by a government are considered to be in the private sector as long as they are not substantially funded by the government, e.g., a provincially owned utility company that is intended to be profitable.

Each province has its own privacy legislation that applies to the public sector. Some provinces like Ontario have separate privacy acts for health care providers. Alberta, British Columbia and Quebec have their own privacy acts for the private sector. The United States does not have an overall privacy act at the national level for the private sector. Instead, it uses industry specific legislations. At the national level, the United States has three acts that address privacy to different degrees. They are Health Insurance Portability and Accountability Act, Fair Credit Reporting Act and Electronic Communications Privacy Act.

Most privacy legislations in developed countries revolve around the Safe Harbour framework developed by European Union. The Canadian legislations are based on this framework. PIPEDA imposes the following ten principles on businesses and not-for-profit organizations that are not substantially funded by a government, like a charitable organization:

1. Accountability.
2. Identifying purpose.
3. Consent.
4. Limiting collection.

5. Limiting use, disclosure and retention.
6. Accuracy.
7. Safeguards.
8. Openness.
9. Individual access.
10. Challenging compliance.

An organization's privacy policy should cover these ten principles. Many large organizations post their privacy policies online. The privacy policy of the Bank of Montreal has been extracted and pasted later in this chapter. In addition to privacy, PIPEDA recognizes digital signature. For each of the ten privacy principles, we have outlined the key internal controls organizations should implement to ensure privacy protection.

Accountability

PIPEDA expects each organization to

- designate someone in the organization to be accountable for compliance,
- protect personal information held by the organization or transferred to a third party, and
- develop and implement personal information policies and practices.

Internal Controls

1. Designating a senior employee to be accountable for privacy compliance. In a large organization, this person is called the chief information privacy officer.
2. Develop a privacy policy.
3. Provide this accountable person and the management team with privacy training.

Identifying Purposes

The organization must identify the reasons for collecting personal information before or at the time of collection. This includes the following procedures.

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.

Internal Controls

1. Indicate on forms and the web site the purpose of collection where personal information is collected.
2. Provide procedures to staff members collecting personal information to state the purpose when information is collected verbally or in free form of written communication.
3. Train employees collecting personal information to answer an individual's questions about the purposes of the collection.

Consent

Unless required by criminal law or a similar statute, an organization must obtain consent from the person providing personal information at the time of request for the information and before disclosure. This includes the following procedures.

- Communicate in a manner that is clear and can be reasonably understood.
- Record the consent received.
- Never obtain consent by deceptive means.
- Do not make consent a condition for supplying a product or a service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose.
- Explain to individuals the implications of withholding or withdrawing their consent.

Internal Controls

1. Indicate on forms and web sites that consent is requested and required where personal information is collected.
2. Provide procedures to staff members collecting personal information to obtain and document consent when personal information is collected verbally or in free form of written communication.
3. Refrain from using automated recording of personal information disclosed by customers or employees before cautioning the individuals that such recording will take place, even if the purpose of recording is obvious.

Limiting Collection

The organization must limit the collection of personal information to the purpose for which the information is needed. This includes the following procedures.

- Not collect personal information indiscriminately.
- Not deceive or mislead individuals about the reasons for collecting personal information.

Internal Controls

1. Design forms such that personal information is collected only in consistency with the stated purpose.
2. Provide procedures and templates to staff members to collect only the personal information necessary for the stated purpose.
3. Regularly review personal information in transaction systems to assess relevance.

Limiting Use, Disclosure and Retention

The organization must not use or disclose personal information other than for the purpose of collection and must not retain personal information longer than needed for the purpose of collection. This includes the following procedures.

- Put guidelines in place for accessing, disclosing, retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable period. This should allow the person to obtain the information after the decision and pursue redress.
- Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

Internal Controls

1. Develop a retention schedule for personal information, based on the purpose of collection.
2. Program retention duration in systems to automatically purge data where practical.
3. Provide procedures to employees who come across personal information to specify how the information can be used.
4. Provide procedures to employees who come across personal information to specify how the information can be disclosed and who to disclose to.
5. Train managers about limiting use. For example, in deciding whether to promote someone, a manager can review the absence records in terms of attendance reliability. But s/he must resist the temptation to go to the personnel file to read medical notes that supported absences. Attendance record is not personal information. The medical notes were collected solely to support absences, not to be used to assess an employee's physical or mental fitness for promotion. Medical notes constitute protectable personal information.
6. Configure web servers to be P3P compliant. Platform for Privacy Preferences (P3P) is a security protocol for web sites to declare how they will use the information collected through a browser, in accordance with their posted privacy policy. For example, if a privacy policy says that the organization will not use a cookie to change a customer's data in the PC, the web server logic should be internally certified by the organization that it will not use a cookie for that purpose. Once a web server is configured to be P3P compliant, a browser can check whether the web site is P3P compliant and if so, the browser's configuration can trust the web site more. For example, a browser can be

configured to reject cookies from a web site that is not P3P compliant. How does a browser know that a web site is P3P compliant? P3P is like XBRL in a way. It is a standard for an organization to put its privacy policy in a compact form readable to only a browser. The compact privacy policy contains parameters about privacy, e.g., what kind of cookies and how they will be used.

Accuracy

The organization must implement internal controls to ensure the accuracy of personal information collected, disclosed and retained. This includes the following procedures.

- Keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interest of the individual.
- Update personal information only when necessary to fulfill the specified purposes.
- Keep frequently used information accurate and up to date.

Internal Controls

1. Provide user friendly screens and procedures for capturing personal information.
2. Provide system edit checks such as date format check.
3. Display entered sensitive information like date of birth for user confirmation before recording.
4. Perform periodic verification of personal information with employees and customers.
5. Perform regular backup of personal information.

Safeguards

The organization must implement access controls over personal information. This includes the following procedures.

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

Internal Controls

1. Use access control lists and user profiles to control access.
2. Require users to label documents and data files with sensitivity levels and provide guidelines for determining the sensitivity levels.
3. Use passwords.
4. Encrypt sensitive information like medical records.

Openness

The organization must make its privacy policy available to customers and external stakeholders. This includes disclosing the following:

- name or title and address of the person who is accountable for the organization's privacy policies and practices.
- name or title and address of the person to whom access requests should be sent.
- how an individual can gain access to his or her personal information.
- how an individual can complain to the organization.
- brochures or other information that explain the organization's policies, standards or codes.
- description of what personal information is made available to other organizations (including subsidiaries) and why it is disclosed.

Internal Controls

1. Post the privacy policy on the web site.
2. Make the privacy policy available to customers on request.
3. Put the privacy policy on the organization's annual report.
4. Require the CEO's approval of the privacy policy and any change thereof.

Individual Access

The organization must allow individuals who provided personal information access to the information they provided. This includes the following procedures.

- When requested, inform individuals if the organization has any personal information about them.
- Explain how such personal information is or has been used and provide a list of any organizations to which it has been disclosed.
- Give individuals access to their information.
- Correct or amend any personal information if its accuracy or completeness is challenged and found to be deficient.
- Provide a copy of the information requested, or reasons for not providing access.
- An organization should note any errors and corrections on the file and advise third parties where appropriate.

Internal Controls

1. Put on the web site and the annual report the procedures and contact names for customers and employees to view their own personal information.
2. Provide procedures to staff members to handle customers' and employees' requests for access, including the approval process.
3. Provide procedures for documenting access requests and their disposition.
4. Perform independent review of processed access requests to assess privacy compliance.
5. Provide privacy training to all employees.

Challenging Compliance

The organization must respond to challenges by stakeholders and privacy authorities about the organization's compliance with the respective privacy legislations. This includes the following procedures.

- Develop simple and easily accessible complaint procedures.
- Inform complainants of avenues of recourse. These include the organization's own complaint procedures and the privacy commissioner.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

Internal Controls

1. Develop procedures for handling complaints from the privacy commissioner, customers and employees.
2. Provide procedures for documenting such complaints and their disposition.
3. Conduct periodic management review of outstanding complaints and complaints that have been addressed to assess privacy compliance.

Sample Privacy Policy

The following is the privacy policy of the Bank of Montreal, a major Canadian bank.

Your Privacy is our Priority

This Privacy Code outlines our commitment to you and is designed to comply with applicable Privacy legislation in Canada, which incorporates the following ten (10) principles:

Accountability

Identifying Purpose

Obtain Consent

Limit Collection

Limit Use, Disclosure and Retention

Be Accurate

Use Appropriate Safeguards

Be Open

Give Individuals Access

Provide Recourse

1. Accountability

Each and every one of our employees is responsible for maintaining and protecting the personal information to which they have access. We have strict policies and procedures for protecting personal information and designated individuals within BMO Financial Group who are responsible for monitoring our compliance.

BMO Financial Group has a Chief Privacy Officer who oversees privacy governance including policy, dispute resolution, education, communications activities and reporting to our Board of Directors and Executive Management on enterprise-wide privacy matters. See principle #10 for contact information.

2. Identifying Purpose

When you become a BMO Financial Group customer, or apply for additional products and services, we ask you for your personal information for the following purposes:

- to verify your identity and protect against fraud,
- to understand your financial service requirements,
- to determine suitability of products and services for you,
- to determine your eligibility for certain products and services, or those of others, and offer them to you ,
- to set up and manage products and services you have requested, and
- to comply with legal or regulatory requirements

Your personal information may be verified with credit bureaus, credit insurers, registries, your employer, personal references and other lenders.

3. Obtain Consent

When you apply for a new product or service, we ask you for your consent to collect, use or disclose your personal information. You may, at any time, withdraw your consent as long as:

- you provide reasonable notice;
- we are not legally required to collect, use or disclose your information; withdrawing your consent does not impede our ability to fulfill your contract with us;
- it does not relate to a credit product we have granted you where we are required to collect and exchange your personal information on an ongoing basis with credit bureaus, credit insurers and other lenders.

4. Limit Collection

We only collect the information we need. We may ask you to provide the following personal information: Social Insurance Number (SIN) for tax reporting purposes as well as other government purposes, such as when opening an income generating account or a registered retirement investment. We do this in order to comply with the Canada Revenue Agency's income reporting requirements. We may also collect and use your SIN for administrative purposes, such as to ensure an accurate match between your personal information and your credit bureau information, or as an internal identification number to accurately identify customers having same or similar names. Financial Information to ensure that the advice we give is appropriate for you and/or the investments you purchase are suitable for your circumstances. Health Information is required for some of our insurance products to ensure that you are eligible for coverage. Contact Information such as your name, address, telephone number or email address.

You can choose not to provide us with certain information in some situations. However, if you make this choice, we may not be able to provide you with the product, service, or information you request. We may monitor or record our incoming or outgoing telephone calls with you for our mutual protection.

We will make certain that you are informed of the purposes listed above when you apply for any of our products or services. If a new purpose for using your personal information develops, we will ask you for your consent.

5. Limit Use, Disclosure and Retention

BMO Financial Group will only use or disclose your personal information for the reason(s) it was collected. Under no circumstances do we sell or give lists of our clients to other companies for their own use and, if we obtain client lists from other organizations, we require the organizations to confirm their compliance with all relevant privacy legislation.

Your personal information may be shared with other companies within BMO Financial Group for the purpose of marketing, including telemarketing, so that these companies can offer you a broader range of product and service solutions to meet your needs.

To ensure that you benefit from our full range of products and services, we will, with your consent, or as required by law or regulation, share your personal information amongst BMO Financial Group. Over time, we may buy new businesses or sell some of our businesses. Accordingly, personal information associated with any accounts, products or services of the business being purchased or sold will be transferred as a business asset to the new business owner.

We may use other companies to provide services on our behalf such as data processing, account administration and marketing. They will be given only the information needed to perform those services. We have contracts in place holding these companies to the same high standards of confidentiality by which we are governed. In some cases, these other companies may be located outside Canada and may be required to disclose information to government authorities, regulators or law enforcement under a lawful order made in that country.

Personal information may be released to legal or regulatory authorities in cases of suspected money laundering, insider trading, manipulative or deceptive trading, or other criminal activity, for the detection and prevention of fraud, or when required to satisfy the legal or regulatory requirements of governments, regulatory authorities or other self-regulatory organizations. Other reasons for the release of personal information include when we are legally required to do so (e.g. by court order) or to protect our assets. If we release personal information for any of these reasons, we keep a record of what, when, why and to whom such information was released.

BMO Financial Group has policies in place that govern the retention of your personal information so it will be kept only for as long as it fulfills its intended purpose or as legally required.

6. Be Accurate

We are committed to maintaining the accuracy of your personal information and ensuring that it is complete and up-to-date. If you discover inaccuracies in our data, or your personal information changes, please notify the branch or office where you do business immediately, so that we can make the necessary changes. When required, we will make our best efforts to advise others of any important amendments to your personal information that we may have released to them. If we do not agree to make the amendments that you request, you may challenge our decision. Recourse is described in principle #10.

7. Use Appropriate Safeguards

Your personal information is secure within BMO Financial Group, regardless of the format in which it is held. We have comprehensive security controls to protect against unauthorized use, access, alteration, duplication, destruction, disclosure, loss or theft of your personal information.

We maintain physical, electronic and procedural safeguards to protect your personal information. Examples of safeguards include restricted access to our information processing and storage areas, limited access to relevant information by authorized employees only, use of passwords, PINs and pass keys, firewalls and encryption of electronically transmitted information, and the use of secure locks on filing cabinets and doors.

We have agreements and controls in place with credit bureaus, credit insurers, other lenders and third party service providers requiring that any information provided by us must be safeguarded and used only for the sole purpose of providing the service we have requested the company to perform.

Within BMO Financial Group web sites, cookies or other information-tracking technologies may be used to improve the functionality or security of web sites, or to provide you with a more customized online experience. Please note that cookies cannot capture files or data stored on your computer. Refer to BMO's Web Tools Statement for further details regarding information-tracking technologies.

8. Be Open

BMO Financial Group's Privacy Code is available in our branches and offices as a printed brochure. From time to time, we may make changes to this policy and will inform you of changes, as required by law. The most up-to-date Privacy Code, is always available at www.bmo.com and the privacy link located at the bottom of the page.

9. Give Individuals Access

If you want to review or verify your personal information, or find out to whom we have disclosed it, please request this by contacting the branch or office where you do business. We may need specific information from you to enable us to search for, and provide you with, the personal information we hold about you. We may charge you a nominal fee depending on the nature of your request. However, we will advise you of the fee prior to proceeding with your request. There may be instances where we are unable to provide some of the personal information we hold about you and if we are unable, we will let you know the reason(s) why.

In most provinces you have the right to access and verify the personal information held about you by credit bureaus. We will provide you with the name and location of any credit bureau that has provided us with a report on you.

10. Provide Recourse

The branch or office where you do business is well equipped to handle any questions you may have about our Privacy Code. However, we want to hear from you if you have any further concerns. Please contact us at one of the following offices:

President and Chief Executive Officer
Personal and Commercial Banking Canada
BMO Financial Group
P.O. Box 1
1 First Canadian Place
Toronto, Ontario M5X 1A1
Call: 1 800 372-5111

Or

President and Chief Executive Officer
Private Client Group
BMO Financial Group
P.O. Box 150
1 First Canadian Place
Toronto, Ontario M5X 1H3

Or

Chief Privacy Officer
BMO Financial Group
P.O. Box 150
1 First Canadian Place
Toronto, Ontario M5X 1H3

Independent Oversight

Office of the Ombudsman
BMO Financial Group
55 Bloor Street West
Toronto, Ontario M4W 3N5
Call: 1 800 371-2541
Or
Fax: 1 800 766-8029
Or

Office of the Privacy Commissioner of Canada
Place de Ville, Tower B, 3rd Floor
112 Kent Street
Ottawa, Ontario K1A 1H3
Call: 1 800 282-1376
Or
Fax: (613) 947-6850

Respecting Your Privacy Preferences

BMO Financial Group fully respects your privacy preferences. Simply contact the branch or office where you do business to discuss the following options that are available to you:

Direct Marketing - If you do not want to receive direct marketing communications, please ask us to remove the personal information about you from our marketing lists.

Sharing - If you do not want us to share personal information about you among BMO Financial Group members (see Scope for list of members), request to opt out of this type of sharing. Please note that you cannot opt out of sharing your personal information where you have requested a product or service that is jointly offered by more than one member of BMO Financial Group or when the sharing is required by law or regulation.

Social Insurance Number (SIN) - If you do not want us to use your SIN for administrative purposes as described in principle #2, with the exception of income tax reporting or other legal or regulatory purposes, request to opt out.

Source: http://www.bmo.com/home/about/banking/privacy-security/our-privacy-code; accessed on March 5, 2014.

INTELLECTUAL PROPERTY

Organizations that increasingly offer eBusiness tend to use and own more intellectual property. For example, a major Internet pure play company in the world has intangible asset that accounts for about 14% of its total asset. Its search engine gives it a significant competitive edge. Intellectual property is subject to the following risks:

- Inaccurate valuation because the property is obsolete, the associated legal agreement is flawed, or the business environment has deteriorated.
- Infringement thereby affecting the company's competitiveness.
- Loss of software and documentation resulting in a company's inability to apply the intellectual property.
- Incurring legal claims that the company has infringed on another company's intellectual property.
- Ownership dispute; for example, does a consultant have software copyright or does the company which hired the consultant have it?

Legal disputes and protection of intellectual property are increasingly prevalent. This has given rise to a new area of legal practice, intellectual property law. The legal implications affect financial statement presentation in terms of valuation and contingent liability.

Common Intellectual Properties

The following types of intellectual property are common in large companies, especially companies whose business increasingly rely on the Internet. They should be protected with rigorous contracts, code of business conduct, user education, registration with the appropriate government office, access control and monitoring.

- Patent, such as a search engine or an advanced computer chip. Technology companies own a lot of patents that keep them competitive. Many company acquisitions are carried out because of the value of patents. A patent is granted only if it is invention in nature.
- Copyright, e.g., for software. Copyright does not have to be granted by the government. It can be registered with the government of origin. Registration is not necessary for copyright to be legally defensible, but registration enhances legal enforceability as it puts others on notice that the copyright has been accepted by the government.
- Trade secret, e.g., business plan, product strategy.
- Trademark, e.g., a well known domain name that has significant commercial value, like google.com. Another example of trademark is Apple computer. Trademark does not have to be registered to be defensible. For a trademark to be defensible, the owner must demonstrate that an alleged infringing party uses the same or highly similar name for the same or highly similar business. A trademark distinguishes the trademark owner from others like competitors in terms of reputation and goodwill. Trademark infringement is called "passing off". In order to sue for passing off, the trademark owner has to prove the following.

1. The owner has acquired a reputation in association with the trademark.
2. The defendant has misrepresented to the public so as to cause deception or confusion between the owner and the defendant.
3. Damage has been or likely will be caused to the owner.

Registration deters infringement and strengthens an organization's position to seek legal recourse; it is a moderately preventive control. Access control, which we will discuss in Chapter Eight, serves as a stronger type of preventive control as it prevents access by unauthorized parties. Monitoring of the use of intellectual property by employees and customers serves as a detective control, e.g., reviewing access logs and Internet activities related to or resembling the organization's intellectual properties. The latter is difficult and time consuming, but some reasonable effort should be taken. Some large companies devote staff resources to perform this kind of Internet monitoring. Employee education about safeguarding is also important.

Intellectual Property Controls

The following internal controls should be implemented to protect intellectual property.

- Registration with government intellectual property offices
- Inventory of intellectual property
- Access controls
- Confidentiality agreement with employees and consultants
- Management review of consultant activities
- Assignment of copyrights in consultant contracts
- Waiver of moral rights in consultant contracts
- Software license agreement
- Source code escrow agreement
- Digital right restriction by putting locks on document features like copying and printing.
- Management review of access logs
- Monitoring of Internet activities to detect infringement.

Intellectual Property Registration

Registration of intellectual property deters infringement and puts the copyright owner in a better legal position to seek compensation for damage because a public and legal notice has been declared about ownership. In Canada, intellectual property can be registered with Canadian Intellectual Property Office or the Canadian Patent Office.

- Copyright is registered in accordance with the Canadian Copyright Act and the protection will survive the author by 50 years.
- Trademark registration is valid as long as it is regularly renewed and the trademark continues to be used for the purpose stated during registration.
- A patent gives the patent owner 20 years of protection from infringement, under the Canadian Patent Act.

MANAGEMENT CHECKLIST

To ensure that eBusiness and EDI are effectively controlled including compliance with privacy legislations, management should apply the following minimum checklist.

1. Develop an eBusiness strategy that is congruent with the overall business strategy.

2. Obtain board approval of the eBusiness strategy.

3. Develop an eBusiness policy and standards that address authorization, accuracy, information sensitivity and security.

4. Develop an information privacy policy and post it on the web site.

5. Appoint a chief information privacy officer.

6. Review contracts with Internet service providers annually to ensure adequate provision for responsibilities, billing arrangements, security and privacy.

7. Train eBusiness developers, operators and managers on eBusiness and privacy legislations.

8. Ensure EDI arrangement with each trading partner is documented in the form of a contract.

9. Thoroughly test each new EDI interface.

10. Keep accurate inventory of intellectual property and periodically assess whether valuation is realistic and conservative. Periodically assess and test the protection mechanism for intellectual property.

CONCLUSION

eBusiness is here to grow. Not many people will dispute this. While today's eBusiness customers are more at ease with the Internet than customers ten, twenty years ago, there remain significant risks with respect to transaction authorization, completeness of audit trail and privacy. In fact, the concern about privacy is higher now than ten, twenty years ago. Organizations that offer eBusiness have to be constantly aware of and regularly assess the risks of unauthorized, illegitimate, inaccurate, incomplete and untimely processing of transactions, as well as the need to protect information privacy. Those organizations that implement sufficient internal controls to mitigate these risks will not only serve as respectable corporate citizens, but also lay a solid foundation for business growth as customers are increasingly IT savvy and demanding with respect to information reliability, integrity and privacy.

SUMMARY OF MAIN POINTS

eBusiness Infrastructure

- Web server, application server, authentication server and database server. all require protection with firewalls and rigorous operating system configuration. The inner servers after the web server need more protection.
- Web master, the person who maintains the web server content, needs to be trained and monitored.
- Routers route traffic from workstations to servers and the Internet. They need to be tightly configured.
- Contracts with the ISPs should be detailed, reviewed regularly and monitored.
- Domain name servers have to be protected from hacker attack to redirect traffic.
- IP address subscription should be optimized to avoid running out of addresses while without paying for unnecessary addresses.

Privacy Principles

1. Accountability – an organization should designate someone to be accountable for privacy.
2. Identifying purpose – When collecting personal information, an organization should state the purpose.
3. Consent – personal information should be collected with consent.
4. Limiting collection – An organization should collect only the personal information needed for the purpose stated.
5. Limiting use, disclosure and retention – In relation to the personal information and the purpose for which it was collected.
6. Accuracy – An organization should put in place a process to ensure the accurate recording and transmission of personal information.
7. Safeguards – An organization should put in place a process to protect personal information.
8. Openness – An organization should be open about its privacy policy and practice.
9. Individual access – An organization should allow the owners of personal information to access the respective information.
10. Challenging compliance – An organization should be prepared to respond to challenges from privacy regulators and individuals who provided personal information.

Electronic Commerce Act

This act is consistent with most eBusiness legislations in other jurisdictions. This Act has following main points.

- It recognizes human-machine interfaces as offer and acceptance.
- It recognizes digital signatures.
- It places the onus on merchants to implement reasonable internal controls to prevent errors made by customers.
- It does not recognize biometrics.

Radio Frequency ID

RFID expedites transactions and helps organizations perform better tracking of assets. However, because of its mobility, the risks of unauthorized transactions, device tampering and privacy intrusion increase. To mitigate these risks, management should consider adopting the following control practices.

1. Review the RFID application project plans and system functions with the chief privacy officer to ensure compliance with privacy regulations.
2. Subject RFID systems and devices to rigorous system integration testing and user acceptance testing.
3. Periodically perform network penetration testing to assess the exposure to hacker and worm attacks.
4. Perform regular physical check of devices.
5. Perform regular testing of data capture and tracking to ensure accuracy.
6. Frequently validate the inventory of activated RFID devices.
7. Regularly review reports of activation and deactivation to ensure tag movements are authorized.
8. Regularly review statistics about tag data transfer volume and delays.
9. Ensure servers have adequate intrusion detection and virus detection software.

10. Deploy network transmission integrity checking techniques like redundant data check.

11. Educate customers and employees about privacy risks and measures to protect their privacy when using RFID, e.g., remove the RFID tag when a suit is sold and do not carry unused RFIDs around.

12. Perform cyclical and year end inventory count instead of relying only on the inventory information on RFID tags.

Electronic Data Interchange

- Electronic transfer of accounting documents using the ANSI or EDIFACT standard, including payments via banks.
- Each organization needs to buy or develop translation software to convert local format to ANSI or EDIFACT format and vice versa.
- Organizations should acknowledge completeness of transfers.
- EDI calls for strong access and reconciliation controls.
- EDI reduces the cost of ordering and therefore lowers inventory level and accounts payable, resulting in less obsolescence and lower cost of storage. A smaller balance sheet means less substantive testing but more control testing, mainly EDI controls.

Controls over Intellectual Property

1. Access control.
2. Contracts and service agreements.
3. Confidentiality agreement.
4. User education.
5. Management monitoring.
6. Registration with government office, e.g., registering patents.

REVIEW QUESTIONS

1. What is the similarity between PIPEDA and Electronic Commerce Act?

2. Which risk does eBusiness affect the most?

3. What is the consequence if a domain name server is hacked?

4. What are the audit implications of EDI?

5. What is the difference between URL, IP address and MAC address and what are the risk implications?

6. What are the risk implications of RFID?

7. What are the key controls to protect intellectual property?

8. How do you think the audit of Google differs from that of General Electric?

9. How does eBusiness affect the five system components of infrastructure, software, people, procedures and information?

10. Referring to the general controls discussed in Chapter Three, which types do you think are more affected by eBusiness?

CASE #1 – Medical Claims Processing

York Life Insurance Company maintains a web site that is used by employers, employees of organizations that subscribe to group medical insurance, dentists, pharmacies, hospitals and other medical service providers to submit transactions and perform enquiries about their policy coverage and claims. Some professional associations and trade unions are also customers, in which case, their members are insured and can submit claims. Claims can be submitted online or by mail. Payments may be made by cheques or direct deposits. If the insured consents, payments may be made directly to the service providers.

Insured individuals can change their coverage options, but they have to go through their employers or trade associations. Insured individuals can check their coverage, entitlement balances and claim history directly by logging onto York's web site.

In addition to claims submission via York's web site, York has launched a chip based coverage card that pharmacies and dentists can insert to card readers attached to their PCs to submit claims. Each insured individual gets such a card. This card helps prevent unauthorized use of cards that are lost, because the insured is required to key in a PIN, unless the claim amounts to less than $50.

The chip based card was launched within the past year after the CIO received many complaints about privacy breach and changes to profiles of the insured without their authorization. He has retained your firm, a Big Four accounting firm, to review the controls over the online claim processes.

Required

Discuss the risks faced by York in offering these web based services and for each risk, suggest a preventive control and a detective control.

CASE #2 – Privacy Policies

Research the privacy policies of three public companies from different industries. For each policy, describe an IT related control that the company should use to support each privacy principle. For each principle, use a different control for each company. One of the companies should be an Internet pure play, i.e., it does not sell products through a physical store or to wholesalers. Another one of the three companies should be a financial institution (bank or insurance company).

RUNNING CASE – Blackberry

Research the patents held by Blackberry and assess the risks with respect to fair value and potential obsolescence.

MULTIPLE CHOICE QUESTIONS

1. Which of the following violates the Personal Information Protection and Electronic Documents Act?
   A. A professor shares your grades with other professors in your university.
   B. A bank uses an employee's doctor notes to assess whether to approve the employee's loan application.
   C. A life insurance company asks about your medical history.
   D. A government job application form asks about your citizenship.

2. Which of the following has the most privacy impact?
   A. Intellectual property
   B. Cookie
   C. Sarbanes-Oxley Act
   D. Database management system
   E. Enterprise resource planning system

3. What does P3P automate?
   A. Privacy policy
   B. Password change
   C. Cookies
   D. Favourite web sites
   E. Web history blocking

4. Which type of controls does the Electronic Commerce Act affect the most?
   A. General
   B. Access
   C. Input
   D. Processing
   E. Application

5. If a bank does not post its privacy policy on its web site, which principle is it violating?
   A. Accountability
   B. Limiting use
   C. Openness
   D. Individual access

6. Which of the following is most likely to occur if a domain name server breaks down?
   A. Business transactions can be decrypted by unauthorized parties.
   B. Users will be spammed.
   C. Users transactions cannot be forwarded.
   D. User computers will be infected.

7. Which of the following types of intellectual property is infringed on when someone distributes purchased music to a large group of friends?
   A. Patent
   B. Trademark
   C. Copyright
   D. Goodwill

8. Which type of control does intellectual property registration belong to?
   A. Corrective
   B. Preventive
   C. Detective
   D. Restrictive

9. Which organization is subject to PIPEDA?
   A. A Canadian bank
   B. University of Toronto
   C. Government of Ontario
   D. Toronto Hospital
   E. Department of National Defence

10. Which risk do EDI payments mitigate?
   A. Late payment
   B. Overpayment
   C. Underpayment
   D. Paying the wrong party
   E. Bounced checks

CHAPTER SIX – APPLICATION CONTROLS

"*Drive thy business, let not that drive thee."* - Benjamin Franklin

Every CEO would agree to the above statement. Driving means moving ahead with a plan. A driver has to know where to go, stop and turn as well as how to control the car. It is the last function, control, that keeps the car progressing in a direction that the driver wants. Driving a business requires controls to ensure that business goals are met efficiently and avoid just going through the motion.

We started our discussion of internal controls in Chapter Three, where we talked about how internal controls should be mapped to inherent risks for management to achieve a tolerable level of business risk. The tolerable level should be set where the cost of an extra control would exceed the cost of the risk if materialized, taking into account the probability of the risk. This is called a reasonable level of internal controls.

An internal control is an established instruction, procedure or tool to mitigate an inherent risk. An internal control is not an essential business activity or procedure for a transaction to complete. This means internal controls are optional for individual transactions although the lack of internal controls in a transaction increases the risk with respect to fictitious transactions, incompleteness, inaccuracy, untimeliness, lack of authorization and inefficiency. In the long run, internal controls are not optional. A system that has insufficient controls is less and less reliable.

To ensure that risk mitigation is organized and coordinated effectively, management should correlate internal controls to provide sufficient redundancy to prevent risks from being ignored while avoiding significant duplication of effort. Such correlation is called a plan of internal controls. This plan should be documented and used as a basis for employee training and regular risk assessment.

Internal controls may be general in nature or specific to applications. A general control is one that is applied to an environment or multiple applications. An application control mitigates the risk of only one system application. It would appear that general controls are more cost effective. However, because applications differ in risks and environments, organizations cannot implement only general controls. Management should start with general controls until the cost of a general control exceeds the monetary impact of the risk being mitigated. Then, if the residual risk is too high and it very much likely will be, application controls should be implemented. Although an application control applies to a specific application (system), the same technique can be used across applications. For example, a credit limit and a check limit both use the same technique, but applied in different contexts.

APPLICATION CONTROL DOCUMENTATION

Application controls should be documented in policies, standards, procedures, system user requirements, design narratives describing work flows, entity relationship diagrams, system flowcharts and programs. For each system, there should be a list of internal controls that can be cross referenced to the documents mentioned above. This list of controls will be used for control and risk assessment of the system as well as for references in audits, control assurance to regulators and training courses.

APPLICATION CONTROL OBJECTIVES

Regardless of the application, there are six generic control objectives. They are: completeness, authorization, accuracy, timeliness, occurrence and efficiency. Internal controls are designed and implemented to ensure that information is reliable.

Internal controls should be applied to each stage of a transaction cycle. The typical transaction cycle includes input, processing, output and data storage. Relating this cycle to the control objectives of completeness, authorization, accuracy, timeliness, occurrence and efficiency, management and auditors can use the following matrix to assess the adequacy of internal controls.

	Completeness	Authorization	Accuracy	Timeliness	Occurrence
Input					
Processing					
Output					
Storage					

Management can complete this matrix for each system and subsystem and rate each cell as high, moderate or low. A low rating is generally unacceptable. When should controls be moderate versus high in reliability and sufficiency? This depends on the degree of inherent risk and materiality of the system. There are software tools to aid in risk and control assessments.

TYPES OF APPLICATION CONTROLS

Application controls can be preventive, detective or corrective. Preventive controls usually give the organization better value for money than detective and corrective controls. However, an organization cannot rely only on preventive controls, otherwise operation will be too constrained. Organizations have to supplement preventive controls with detective and corrective controls.

Here are some common application controls:

- Access controls.
- Aging analysis to estimate inventory obsolescence and uncollectible accounts.
- Automated notifications to management on rate changes, salary changes, new hires etc.
- Batch total to ensure completeness.
- Credit limits.
- Customer statements for customers to verify transactions.
- Data correlation to identify anomaly, e.g., to detect illegitimate transactions or kickbacks.
- Database controls.
- Displaying data entered for the data entry clerk to verify accuracy.
- Exception reporting of transactions for management or independent review.
- Hash total to ensure completeness.
- Input edit checks.
- Management review of significant transactions.
- Run to run control total to ensure completeness.
- Segregation of duties between incompatible functions, between systems and within a system.
- Signing authority limits.
- Validity check of input data by verifying to a table of acceptable values.

Access Controls

Access controls can occur at a general level or an application level. For example, a password can be used to restrict access to the network. Another password can be used to authenticate users of the payroll system. We will discuss access controls in Chapter Eight.

Batch Total

Batch total is a common application control to ensure completeness of data input and processing. Here is an example of how it works.

1. At the end of each business day, a teller collects the checks deposited in an ATM, and prints a list of deposits from the ATM.
2. The teller then keys in the amount of each check through a check clearing machine and feeds the check through the check clearing machine reader.
3. The clearing machine reads the pre-encoded bank number, branch number and account number.
4. The machine also encodes the check amount on the check.
5. When all the checks have been entered through the check clearing machine, the teller prints a list from the machine and compares the total to the ATM total.

6. If they differ, the teller will check the both lists to determine the reason for the discrepancy.
7. Once the two totals balance, the teller will run the "confirm" command on the clearing machine.
8. The check clearing machine will create a file of checks processed and send it to the data center along with the scanned image of each check.
9. The teller will bundle the check with the ATM list and check clearing machine list for storage.
10. The data center sorts the file by bank number and sends a file to each drawee bank with the check images for collection.

A batch total can be applied to amounts or quantities. It can be taken at any stage when source documents are transported to ensure that documents are received in entirety and subsequently entered to the system. This technique basically involves comparing two totals of the same population taken at different stages of the transaction recording cycle to ensure that transactions are recorded completely and accurately. A drawback of a batch total is that it does not detect offsetting errors. In the above example, if a $100 check was not entered to the check clearing system, but another $100 check was entered twice, the two batch totals will still agree and this error will not be detected. To detect offsetting errors, organizations can implement hash totals.

Hash Total

This is similar to batch total. However, instead of keeping track of an item count, quantity or amount, it uses a numeric field that is not intended for calculation. In the above example, in addition to totalling the amount of checks, the ATM could total the account number of each check for subsequent comparison with a similar total generated by the check clearing machine. However, this is impractical because the ATM cannot read the account number of each check because the checks are in envelopes. Thus, hash total is inapplicable.

Hash total is applicable to checks deposited over the counter. When a teller accepts a deposit, s/he credits the customer's account. In addition, s/he keys in the account number and amount of each check to a memo file online. At the end of shift, s/he generates a list of checks accepted with an amount total and an account number total. This list is wrapped around the batch of checks for entry to the check clearing machine by another teller. The amount of each check is entered to the clearing machine and the machine reads the encoded account numbers. When the entire batch has been entered, the clearing machine generates a list similar to the one generated by the "memo" system at the teller's wicket. The second teller compares the totals between the two lists. If there is any discrepancy, the second teller will check individual entries to find out why. The hash total can detect offsetting errors between losing a check and keying another check of the same amount twice. However, if a $100 check is entered as $200 and vice versa, neither the hash total nor the batch total will detect these offsetting errors. This shows that batch total and hash

total mainly address completeness and to some extent, accuracy, but other controls are needed to ensure accuracy, such as edit checks or displaying an amount on data entry for the data entry person to verify.

Run to Run Control Total

There are many programs and functions in a system that process transactions. A transaction often has to go through many functions before it is fully processed. A system may pass transactions in batches from function to function. Just as it is important to pass control totals when source documents are transported, it is useful for functions in a system to calculate "batch totals" within a system for the receiving function to verify that all transactions that should have been passed between system functions have been received. For example, in an enterprise resource planning system of a company with diversified business units, payroll transactions information is transmitted to work-in-progress inventory of the applicable business units. In addition, the total of each day's payroll transactions applicable to a business unit is transmitted. The inventory system receiving the transmission of payroll information will first calculate a total of the payroll costs for the day being transferred and then compare the calculated total with the transmitted total. Once the two totals agree, the inventory system will apply the detailed data to work-in-progress inventory.

Segregation of Duties

The purpose of segregation of duties is to provide opportunities for errors to be detected and to reduce the opportunity for irregular practices or fraud. It is critical to segregate the duties of IT from businesses. This is segregation of duties at a general level. It is similarly important to segregate incompatible functions in the business and accounting areas. Two functions are incompatible if they satisfy the following criteria:

- Having one person performing both functions will unduly and significantly increase the risk of fraud or undetected errors.
- Assigning the functions to at least two persons will not significantly impair operation effectiveness or efficiency.

Segregation of duties is therefore based on risk assessment. Where it is impractical to segregate duties because of staff constraint, the organization can mitigate the resultant risk with more rigorous exception reporting and management review. For example, in a small organization, because of a maternity leave, if the controller who approves invoices is told to also approve purchase orders, the president can mitigate the increase in risk by reviewing all large payments after processing for substantiating documents. Segregation of duties should be implemented via organization charts, procedures, job descriptions, training and access controls.

Input Controls

This is the first series of internal controls to be applied to a transaction, to ensure that input reflects real transactions, is complete, authorized, accurate, timely and efficient. Controls should be exercised to assess whether data input is supported by a legitimate business transaction, including internal operational transactions. An example is assessing whether hours entered reflect actual hours worked by verifying to time sheets or asking a supervisor to review hours entered. Input controls may be manual or automated, they may also be in real time or a delayed mode. An example of a real-time control is for the system to check the data entered before accepting it. An example of a delayed control would be validating the data after accepting entry but before processing. An input control must be applied before processing, otherwise the purpose of the control is nullified.

Edit Checks

A common technique in input control is edit check. For example, an invoice with a negative amount should be reviewed before the sales journal and the accounts receivable subsidiary ledger are updated. Here is a list of common edit checks.

- Check digit, last digit of a control number serves as a control digit to validate the number. This is commonly used in government service program eligibility numbers like social insurance and social security numbers.
- Data format check, e.g., a date field should be yyyymmdd.
- Limit check.
- Missing data check, i.e., all mandatory fields are filled in.
- Range check.
- Sequence check
- Sign check.
- Validity check, by verifying data input to a table of acceptable values.

Input Controls to Ensure Completeness

Transactions are often not processed properly because data is input incompletely. Here are some controls to mitigate this risk.

- User friendly screen to avoid incomplete data entry.
- Make certain fields mandatory and enforcing this with a system feature.
- Procedures to indicate the requirement to enter all fields.
- Emphasize mandatory field entry in user training.
- Batch control total comparing the total of amount or quantity from source documents to the total of amount or quantity input to the system.
- Hash total comparing certain arbitrary numeric fields from source documents to the corresponding fields input to the system.
- Display input screen after data entry to the employee or customer and asking for confirmation.

- Document count control comparison before and after data entry.
- Audio repeating of data entered to the customer.
- Summary screen displaying total value of key fields entered for confirmation by the employee or customer.

Input Controls to Ensure Authorization

A user who has been granted access to a system for data entry can enter any data if there are no controls to restrict and detect the entry of data without authorization or the entry of invalid data. Here are some examples of application controls to ensure authorized data entry.

- Access to dormant bank accounts requires supervisor override. A bank classifies a deposit account as dormant when there has been no customer initiated transaction for two years. Any human initiated transactions like a deposit, withdrawal or transfer made to a dormant account should trigger an alert to the branch manager, and if the initiation is done by the branch manager, the alert should be directed to the area manager.
- Authorized documents for data input are made available to only restricted employees.
- Data entry in excess of a certain limit in transaction amount requires a supervisor's override, also called management override.
- Input of highly sensitive data requires the involvement of at least two employees.
- Online bank account creation by a customer is not fully processed until a client returns a signed agreement.
- Online system displaying only human readable data and asking for the data to be entered along with the transaction data to confirm that data entry is performed by the authorized person, as opposed to being faked by a hacker's program. For example, the customer is shown a character string in different highly italicized fonts and asked to type in the string. This control is intended to prevent automated data entry engineered by a hacker.
- Online transaction input is routed to another employee to confirm with the customer before processing.
- Management overrides are logged and reported for more senior management review.
- Senior management review of management overrides is also logged for audit trail.
- Procedures require the examination of management authorization before data entry.
- System asking for a ticket number or authorization number before accepting data.
- System notifying the appropriate managers of certain sensitive data entered before processing to seek confirmation of authorization.

Input Controls to Ensure Accuracy

Data entry is error prone. This is one of the reasons organizations increasingly automate data capture at source. Automated data capture also saves time. Here are some input controls to ensure accuracy.

- Applying a check digit to validate the entry of a control number like a product number. The check digit is the last digit of the number. For example, for product number 123456, a check digit, say 7, is added to the end. When an employee enters 1234567, the system applies a formula to 123456 to calculate the last digit. If the calculated value is 7, the data entry is accepted because the number satisfies the formula. If the data entry person makes a mistake in that number, the last digit will highly likely to be a value other than 7 and the system will not accept it. The reliability of this method depends on the length of the number and the sophistication of the formula. This method only helps ensure valid, but not necessarily correct data entry. In other words, even if a number satisfies the formula, it may not be the intended number; for example, an employee may enter the product number for a bicycle instead of a tricycle. A common application of check digit is for the creation of bar codes for products. If a staff member enters an invalid product number, i.e., one that does not exist in the inventory system and if the number has been turned into a bar code, that product will require a cashier to call someone to go to the shelf to check the actual price because the bar code will not be accepted by the inventory system. A check digit formula can be applied by the system to check that the number entered to the bar code creation system is valid so that the code inscribed or labelled on products will be acceptable to the inventory system. The check digit method is also commonly used in government social program number like social insurance and social security numbers. Banks also use this method for validating credit card and debit card numbers. It should be noted that a check digit actually forms part of the permanent document or record control number, unlike an error detection value to detect a data transmission error, which is discarded after verification of data transmission.
- Apply data reasonableness check, e.g., is the pay rate reasonable in relation to the staff classification?
- Apply a sign check to detect values that should not be negative.
- Limit check.
- Check for proper data format, e.g., date, numeric and alphanumeric.
- Detailed procedures for data entry to prevent mistakes.
- Display the data scanned to be confirmed by the person doing the scanning.
- Test bar codes for correctness before producing the codes, e.g., assign an employee to read the product description by scanning the bar codes before making the codes "official".
- Test the scanners for accuracy.
- Staff training to prevent mistakes.
- User friendly screen to prevent mistakes.
- Require keying of high value and low volume items by a second person.

Input Controls to Ensure Timeliness

Information may be correct but useless because it is too late. Here are some input controls to ensure timeliness.

- A schedule to ensure timely data entry.
- Audible alarm to remind about data entry.
- Automated data capture.
- Data entry format printed on transaction documents.
- Email reminder for data entry.
- Incentive for early data entry.
- Metrics on timeliness of data entry.
- Place data entry as close to transaction origination as possible.
- Timeliness of data entry included in performance and outsourcing contracts.
- Use radio frequency identifier (RFID) to ensure timely data capture.

Input Controls to Ensure Occurrence

There is a risk that data entered to a system does not reflect real business transactions. To mitigate this risk, management should implement internal controls to validate data, preferably before it gets into the system. The controls can be automated or manual. Automated controls usually entail checking input data to existing data or correlating data from different sources including source documents. Manual controls mainly involve vouching input data to source documents.

Here are some examples of input controls for occurrence, i.e., to confirm that the data entered reflects a real and genuine transaction.

- A cruise company checks for any existing and identical reservation to confirm that it is not a duplicate before reserving the seats.
- A documented procedure that requires the payroll administrator to check for management authorization and employee identification before setting up a new employee in the payroll system.
- A telephone company requires a second employee to call the customer back to confirm an order.
- An insurance company checks for effective coverage before accepting a claim.
- An online stock brokerage alerts a customer when the number of shares of a stock to be purchased equals the number of shares already held, to confirm that the customer actually wants to buy instead of selling.
- Check for existence of a purchase order and shipping documents before accepting invoice data for invoice generation.
- Check the serial numbers of computers entered for disposal.

- Reconcile EDI totals to source system totals before translation to ANSI or EDIFACT format.
- Validate the social insurance/security number upon data entry.
- Validate automated teller machine (ATM) card before allowing transactions to be entered.

Processing Controls

Reliable data input does not guarantee reliable information produced by the system. How data is processed has to be controlled. Increasingly, the input of one transaction can trigger multiple related updates to different systems without human intervention, such as in the case of an enterprise resource planning system (ERP). It is critical that there are sufficient processing controls to ensure transaction processing is legitimate (occurrence), authorized, complete, accurate, timely and efficient.

Processing Controls for Completeness

Here are some internal controls to ensure that transactions are processed completely.

- Batch total and hash total.
- Run-to-run control totals for the system to check the completeness of transactions passed from one program to another.
- Network transmission controls such as parity checks and redundant data checks.
- Reconciliation from subsidiary ledger to the general ledger.
- Reconciliation from transaction journals to the subsidiary ledgers.
- Customer statements.
- Transaction receipts to confirm processing.
- Gap detection to alert management of potentially missing transactions.
- For systems where almost all of the master file records are expected to be updated in each cycle, e.g., payroll, have the system produce a report of any records that do not receive an update.
- A schedule of batch updates to ensure complete processing.
- Confirmation with customers to ensure each transaction is completely processed.

Processing Controls for Authorization

Even with authorized data entry, transactions may still be processed without authorization. For example, a programmer may alter a system function to cause unauthorized processing. Another example is the filling of sales orders that exceed credit limits. Here are some controls to ensure that processing is authorized.

- Confirmation with customer after data entry but before processing to ensure authorization.
- Customers are informed of system generated transactions to ensure authorization.

- Establish and periodically review credit limits.
- Online confirmation with the line manager whose cost center is being charged to ensure authorization before the transaction is processed.
- Procedures require changes to transaction processing schedules or fee arrangement to be approved by customers and management.
- Produce an exception report on sales that have caused credit limits to be exceeded.
- Statistical analysis of processing results to identify unusual trend.
- System generated transactions that are out of the ordinary have to be approved by management before being finalized.
- System renewal of billing arrangement or contracts are approved by management and the customers before being finalized.
- Perform process logic check behind the web interface to detect unauthorized change by a hacker.
- Analyzing the amounts and dates of cash receipts in relation to the outstanding balances and due dates at the time of posting, taking into consideration new purchases that would not yet be due for payment, generally 30 days from invoice dates. This will serve to detect lapping as the fraudster may not find customers that have the exact balances of the customers whose payments have been diverted and also the customers whose payments have been misappropriated would usually be shown by the accounts receivable system to have missed the due dates by a day or two because of lapping.

Processing Controls for Accuracy

Correct input of data may still lead to incorrect transactions if processing or data transcription is wrong. It is critical to have extensive processing controls to verify data transmitted, transcribed and calculated. The following are some key processing controls over accuracy.

- Display the final data to be processed before a transaction is recorded on the screen for user or customer confirmation.
- Data transmission controls like parity check and redundant data check.
- Sequence check and gap detection.
- Statistical checks to assess reasonableness of calculated amounts.
- Limit check.
- Run-to-run control totals.
- Batch and hash totals.
- Three way matching of the purchase order, receiving report and invoice before payment.
- Sign check of quantitative data items to detect negative value that is not right.

Processing Controls for Timeliness

Operation is often delayed because transactions are not processed promptly. This can result from human errors, oversight, system breakdown or network latency. Here are some key processing controls to address timeliness.

- A processing schedule to ensure timeliness.
- A schedule of month end closing.
- Aging of suspense items for follow-up.
- Database error recovery procedures; this will be further discussed later in the chapter.
- Email notification to operators to initiate processing.
- Management review of aged list of suspense items.
- Management review of process logs.
- Periodic analysis of transaction throughput time.
- Staff training.
- Survey with users about timeliness of processing.

Processing Controls for Occurrence

Here are some examples of processing controls to ensure that data is processed only based on real transactions.

- A bank system putting a "hold fund" flag on an account for deposits until the checks have cleared.
- Attach cameras to RFID readers for inventory tracking, to detect tampering or removal of RFID from inventory.
- Cash receipts that cannot be posted to a customer account are recorded in a suspense account for investigation.
- Confirm transactions with customers.
- Confirm with counter-parties before processing a swap. A swap is a two way hedge of a financial instrument like a bond or a commodity trade whereby each of two parties to the swap agrees to cover the variance between the market price and the swap price to "insure" the other party against downturn or upswing. For example, a deal between a nature gas producer and a retailer may agree to a price of $3 per million BTU. If the market price goes to $4 per million BTU, the producer gets $4 from the open market but provides a $1 rebate to the retailer. Conversely, if the market price is $2, the retailer can buy it in the open market for $2 but has to pay the producer $1. What is there to gain by either party? Both are insured against market swings? The producer usually has higher bargaining power because it is the supplier, so the producer usually charges a fee for the swap or builds that into the swap price. That is, the swap price may be a little higher than the expected market price. What is the relevance to computer systems? Systems have been inappropriately used by rogue traders to falsify swaps to hide their unauthorized transactions.
- Direct payroll deposits are reconciled to the payroll transaction file before despatching deposits to the financial institution.
- Duplicate detection to avoid processing a transaction twice.

- System comparison of transactions that are identical in amount, date of service and vendor to prevent processing the same transaction twice.
- Disbursement system cross-referencing to purchase orders before paying invoices.
- Payroll system confirms employee eligibility before accruing vacation credit.
- Payroll system requests confirmation from the hiring manager before creating a file for a new employee.
- Sales system references to original invoices before granting refunds.

Output Controls

Information is reliable only if output reflects real transactions and if it is complete, authorized, accurate, timely and efficient. This requires a combination of system tracking controls, validation checks, management reviews and reconciliations. Because output is increasingly electronic and accessed by users online, some traditional output controls like procedures for report distribution have been replaced with access controls.

Output Controls for Completeness

Incomplete information can lead to incorrect decisions and incorrect financial reporting. What is produced should be checked to ensure all transactions are reflected. Here are some key output controls over completeness.

- A checklist to be signed off once hard copy reports have been distributed.
- Batch and hash totals.
- Confirmation with users to ensure output is received.
- Detailed instructions for interpreting output.
- Highlighted key fields for users to check completeness.
- Management and independent review of processing logs.
- Parity check and redundant data check.
- Procedures to approve changes to distribution lists.
- Reconciliation between systems.
- Requiring users to sign for receipt of paper reports.

Output Controls for Authorization

Even if output is complete, it may be useless or misleading if it is not authorized. Similarly, reports that represent unauthorized transactions can be damaging to the organization. Here is a sample of output controls over authorization.

- A list of authorized users who can sign off reports.
- Guidelines for classifying reports by sensitivity.
- Management review and approval of reports.
- Guidelines for report retention to prevent unauthorized access.

- Guidelines for report shredding.
- Procedures for approval of changes to distribution lists.
- Procedures for approving ad hoc report requests.
- Procedures for management or customer approval of release of information.
- Procedures for securing reports pending pickup.
- Procedures for review and approval of reports.
- System requirement for user review and approval of reports with documented evidence of review and approval via the system.
- A list of authorized report recipients. This control is increasingly being replaced with access controls because more and more output is electronic and available on a "pull" basis. Users may get notification that the output is ready in the system.

Output Controls for Accuracy

Reports must be accurate to be useful. Many users do not realize that the programs used to process transactions are often different from those used in generating reports. This means accurate processing does not necessarily mean accurate output. Here are some key output controls over accuracy.

- Detailed instructions for generating ad hoc reports.
- Highlight totals to make it easy to assess report correctness.
- Instructions for interpreting report.
- Locking key fields on electronic reports to prevent accidental overwriting.
- Parity check and redundant data check.
- Policies and guidelines on end user systems development to prevent incorrect reports.
- Provide users and customers with contact information for reporting discrepancies.
- Reconciliation between systems.
- Separate numerical columns with text columns to prevent misreading.
- Standards for report headings and labels to ensure consistency.

Output Controls for Timeliness

Information may be correct, complete and authorized. But unless it is timely, usefulness can be significantly compromised. Here are some key output controls to ensure timeliness.

- A schedule for producing periodic reports.
- Communicate the report schedule to users so they can question when reports are late.
- Ongoing output is deposited in users' network folders for retrieval.
- Parity check and redundant data check.
- Reconciliation to the general ledger.
- Reminders to users to consider generating ad hoc reports.
- Reminders to users to retrieve reports.

- Reports are generated in real time as much as practical.
- Requirement for users to confirm report receipts.
- User training on the importance of timely review of reports.

Output Controls for Occurrence

Output should be validated to ensure that it reflects real transactions. A transaction may be as simple as an information request. Here are some related controls.

- Accident claim reports are reconciled to traffic tickets.
- Attendance reports are reconciled to timesheets.
- Independent confirmation of insurance policies with customers.
- Invoices are matched to purchase orders.
- Managers receive notification of salary raises related to their subordinates for confirmation.
- Managers review exception reports.
- Managers review payroll transaction reports.
- Sending monthly statements to customers.
- Signatures on printed checks are verified before despatch.
- Stock picking sheets are reconciled to purchase orders.

Application Controls over Stored Information

Information in storage is subject to risks. It may not reflect real transactions because of subsequent manipulation after the initial information is placed in storage. It may be accessed without authorization. It may be changed inaccurately, etc. It is critical to have internal controls over stored information.

Stored Information Controls for Completeness

Stored information may be lost because of inappropriate access or storage media failure. Database maintenance can also affect information integrity. Here are some key internal controls to ensure completeness of stored information.

- Fixed asset verification.
- Frequent review of change logs.
- Periodic audit of database for completeness by vouching to source documents and correlating database tables.
- Periodic confirmation with customers and users.
- Periodically verify the user account list with managers.
- Physical inventory taking.
- Reconciliation between systems.
- Redundant data storage.
- Referential integrity (defined under Database below) checks built in databases.

Stored Information Controls for Authorization

Information stored may be accessed without authorization. The retention of records may go beyond the authorized time periods. Here are some key controls to mitigate the risk of lack of authorization.

- Acceptable use policy. We will discuss this further in Chapter Twelve.
- Assigning data ownership to managers to authorize appropriate controls and access requests.
- Privacy policy.
- Privacy policy compliance checking by doing periodic spot checks.
- Privacy policy training.
- Procedures require approval of changes to record retention schedules.
- Procedures require approval of changes to stored data.
- Procedures require approval of data deletion.
- Procedures specify the process for gaining access to stored data.
- User screens to remind about the need to obtain authorization to share information.

Stored Information Controls for Accuracy

Information stored may, over time, become inaccurate because of media damage or out-of-date procedures. Accidental change can also affect accuracy and integrity. Here are some key internal controls to mitigate these risks.

- Confirmation with employees and customers.
- Database referential integrity check.
- Frequent cross-checking and synchronization of databases.
- Periodic checking of contract information to the latest signed contracts.
- Periodic data tests for unauthorized change.
- Periodic inventory taking of fixed assets.
- Periodic reconciliation between systems.
- Regular review of stored information for obsolescence.

Stored Information Controls for Timeliness

Information stored is not effective if it is not timely. The issue is availability, e.g., is the information available when needed? Is it relevant to the need in terms of the time period it represents? Here are some key controls.

- Conduct user survey about system responsiveness.
- Frequent update of retention schedules.
- Keep track of the dates of updates to assess information currency.
- Label files with expiry dates.
- Regular confirmation with users.
- Regular database synchronization.
- Regular review for currency.

- Regular tests of system availability.
- Regular tests of system queries for responsiveness.
- User instructions for ad hoc reporting and system queries.

Stored Information Controls for Occurrence

Stored information may not reflect real transactions resulting from invalid transactions or change to information after it is initially stored. This risk can also materialize if update or deletion transactions are not processed. Here are some controls to mitigate this risk.

- Changes to dormant bank account balances are reviewed by managers.
- Confirm patent with the government patent office.
- Inventory list is periodically reconciled to physical count.
- Location and assignment of fixed asset are periodically confirmed.
- Periodically confirm that employees on payroll are still employees.
- Periodically purge old data that is no longer required.
- Reconcile the online service catalog to the corporate master list.
- Update databases to reflect organizational changes.
- Verify real estate holdings with the land title offices.
- Vouch recurring charges to contracts.

DATABASE

Databases are increasingly used in organizations to facilitate data sharing for real time transactions and data mining. However, as is common when efficiency is to be gained, risk can go up. The sharing of data files (tables) increases the potential access points and complexity of software. Thus, organizations need to implement controls to mitigate the additional risks. The typical databases used today are relational, object oriented and a hybrid of relational and object oriented models. Relational is the most popular model for systems that process primarily numerical and text data. This allows any two tables with a common field to interrelate and provides a lot of flexibility. In a database, a data file is called a table. A table is visually similar to an Excel spreadsheet. Common relational database management systems are Microsoft's Structured Query Language (SQL) Server and Oracle. Microsoft also has a mini version of relational database management system called Microsoft Access. An object oriented database stores graphical, video, sound and object oriented programming code. An object oriented program is a piece of reusable object code that often contains standard data like font and color. Common simple calculation formulae can also be placed in an object, e.g., for calculating the monthly mortgage payment. It can also contain holders for users to input data, thus combining code and data in one object with the data portion being dynamic. Where the extent of graphic and sound data is limited and such data is often used in conjunction with text and numbers, a relational object oriented database model can be used.

Most business applications use the relational database model.

Database Components

A database is a collection of tables for sharing among applications. A table is also called a file. It consists of fields (attributes) and records. It can be pictured like an Excel spreadsheet where the columns denote the fields and the rows indicate the records.

To control the sharing of tables, the database is driven by a database management system (DBMS). The database management system is a system software product that controls the interfaces of and access to tables. Common database management systems are SQL Server, Oracle, DB2, Dbase, and Microsoft Access. A DBMS also has a data query facility, e.g., structured query language (SQL). The data query facility, or data query language, can be used by transaction processing programs for processing transactions and providing results to standard user queries like an account balance enquiry. The most common command is to select fields, from tables, where (criteria). SQL is also used by programs to insert, update and delete records.

Another component of the database is a data dictionary. The purpose of a data dictionary is to keep track of the tables in a database, what each table contains in terms of fields, the format of each field, and the relative location of the fields in a table. Programs that access a table will go to the data dictionary to find references to the needed tables and fields. The data dictionary must be kept current. It alleviates programmers of the mundane task of keeping track of file names and layout. Programs no longer have to define these to read or write data as the data dictionary serves as the intermediary between programs and the database. For example, a program that wants to read the checking account balance only has to specify the checking account balance field name like CHKBAL as long as only one table has this field name. If more than one table has this field name, the program will qualify the name with the table name, like CHK.CHKBAL. The data dictionary can then go find the table and the value of the field for the specified account number. The data dictionary knows whether the data is numeric or alphanumeric as well as the position and length of the field.

All hardware and software must be managed and controlled by people. The person who controls the database is called the database administrator (DBA). This person configures the database management system, updates the data dictionary and grants rights to programs and users to access tables. The access rights are defined in the DBMS. The DBA has full control of the database. So it is important not to assign more duties to this person. For example, s/he should not be also a system administrator who controls the operating system.

Risks of Database Systems

A database improves efficiency and data redundancy. However, data sharing between applications increases the risk of unauthorized access and update errors. The more programs that can update a table, the more likely errors will occur. Also, because more system software is used in a database environment, the risk of incorrect software

configuration (incorrect parameters) increases. Database applications often are operated in a distributed network. In that case, there are multiple copies of a database geographically dispersed. It is important to ensure that updates are synchronized. It is just as important to ensure time synchronization, by for example, operating a time server. Because a database consists of many tables that are shared between applications, there is also a risk of data inconsistency between tables when data is repeated unnecessarily, e.g., a customer address shows up in multiple tables but is represented inconsistently. This risk results from data redundancy. There is also the risk of concurrent updates, i.e., one transaction overwriting the result of a previous transaction.

Risk of Concurrent Updates

In a database environment, programs sometimes contend for the same table and field in terms of reading and writing. Although technically, the hardware will not allow two programs to update a field at the same time, just as it would be impossible for two full size cars to enter a single car garage, there is a risk of updates performed by two programs almost concurrently that could impair data integrity. Here is an example.

I deposit a $1,000 check at an ATM to a joint checking account. Less than a second later, my wife transfers $2,000 from the checking account to a saving account using eBanking. Before these transactions, the checking account balance is $5,000. Here is what could likely happen.

1. My transaction reads the $5,000 balance and updates it to $6,000.
2. My wife's transaction reads the $5,000 balance (after my transaction has read it but before my transaction finishes) and calculates a new balance of $3,000.
3. My wife's transaction finishes after mine, so it overwrites the new balance as $3,000.
4. In fact, the correct balance should be $4,000.

This is called concurrent update. That is, two transactions update the same field of the same record without knowing about each other. In other words, the left hand doesn't know what the right hand is doing. To prevent this kind of data inconsistency, organizations should configure database management systems to enforce record locking.

Database Anomalies

A table consists of fields and records. A record (row) represents an entity like an employee. A field (column) indicates an attribute about the record, e.g., job title. A table can be very long or very short. For example, all the payroll information can be contained in one table. This will make the table very long and difficult to manage. More specifically, it will present anomalies for record addition, deletion and updates. Here are three examples.

If all payroll information is in one table, it would make sense for the primary key to be the employee number. One of the fields is likely the position number. A position number should be unique for human resources tracking. Sometimes a position is vacant and there will be no associated employee number. Let's say the organization has created a new position that has not been filled. That position cannot be added to the table because the primary key is nil. This is called addition anomaly.

A similar problem is presented if the organization wants to delete a position because it is no longer needed. Because the primary key is the employee number, the organization cannot delete the position as long as the associated employee information has to be kept for income tax purpose. This is called deletion anomaly.

A third problem: If all the payroll information is in one table and the primary key is a combination of the employee number and pay period number, there is a record for every pay period in conjunction with every employee. The employee's address has to be in the system and since there is only one table, the address has to be a field in this table. Because an employee will occupy roughly 26 records per year for an organization that pays bi-weekly, the address will appear 26 times. If it is realized that the address is wrong, the organization has to correct the address on multiple records. Data entry is prone to errors so this risk of data inconsistency is increased. Recording the address on multiple records is called data redundancy. This problem is also called update anomaly.

Database anomalies can be corrected using normalization. Normalization also reduces data redundancy.

Database Controls

The purpose of database controls is to ensure that data access is authorized and that database table integrity is maintained. Integrity means completeness and consistency with other connected tables. We will describe the controls that should be implemented in a database environment to ensure reliability and integrity of information.

1. Segregate the duties of the database administrator (DBA) from other functions.

2. Assign and train backup DBAs.

3. Configure the database management system (DBMS) to enforce the following:
    - Record locking (described below)
    - Referential integrity (described below)
    - Detection and resolution of deadlock (described below)
    - Logging
    - Normalization (described below)

- Synchronization between locations and environments to ensure consistency of content and clocks. Clock synchronization is critical to ensure transactions are time stamped correctly for audit trail and for prioritization of updates and interest calculation (e.g., 11:59 pm vs 12:00 am).
- producing alerts on direct updates, i.e., updating not through an authorized program like ATM, to detect unauthorized data change.
- passwords
- producing alerts on table creation and deletion, to detect unauthorized data creation or deletion.

4. Rotate the duties of database administrators among different environments to increase the opportunity for error detection and reduce the risk of improper practices.

5. Establish procedures for database administration.

6. Establish procedures and authorization levels for approving access profiles for programs and users.

7. Periodic verification of the currency of the data dictionary. By cross-referencing actual table layouts, designed table layouts and entity relationship diagrams to the data dictionary.

8. Establish user procedures for data query to ensure correct applications and interpretation.

9. Establish error recovery and rollback procedures for database corruption or processing halts resulting from network outage, transaction errors or other unexpected occurrences. The DMBS has to recognize when processing was halted or failed and apply data integrity checks to compare before and after images to reconstruct the differences to prevent data loss.

10. Configure the database query facility to prevent someone from running queries to deduce information that the person cannot otherwise obtain directly. For example, someone who does not have access to salary information of specific employees should be disallowed by the system to run successive queries to narrow down to the desired information. Database controls should be enforced in the DBMS to prevent queries that rule out the majority of the population or that focuses on a small part of the population unless the program or the user performing the query already has direct access to the small part being focused or that has not been ruled out. A more detailed description of this example is as follows:

An employee wants to find out how much a female lawyer makes in a firm. If there are only two female lawyers and they have about the same rank and seniority, that person can first query the average compensation of a lawyer. Then he can query the average compensation of a male lawyer. The results of these two queries will give that person what he wants to know.

To prevent the above, the system should not respond to a query where fewer than three records satisfy or do not the criterion, unless the query uses a specific record identifier like employee number. In the latter case, the ability to query is subject to access controls like an access control list, which we will describe in more detail in Chapter Eight.

Record Locking

We have discussed the risk of concurrent update using the bank deposit example, where the withdrawal transaction is not aware of the deposit transaction, leading to an incorrect balance. The principle internal control to mitigate this risk is record locking. Here's how it works.

When a transaction reads a record with intent to update it, the transaction should send a flag to the DBMS so the latter can lock the field where update is intended, and deny it from being read by another transaction until the first transaction has finished. The purpose is to preserve information integrity.

Record locking can lead to a deadlock scenario, i.e., multiple transactions needing to access the same fields of a record for the purpose of updating the record. A deadlock can lead to a standstill as each transaction has to wait for the other transactions to finish. This is further explained below.

Deadlock

When inter-dependent transactions lock multiple records, the system can come to a halt. Here is an example.

- I enter an ATM transaction to transfer $1,000 from a joint checking account to a joint saving account.
- Before this transaction, the checking account and saving account balances are $5,000 and $3,000.
- At the same time, my wife uses eBanking to transfer $2,000 from our joint saving account to our joint checking account.
- My transaction starts first, so it locks the checking account balance after having read it; but before it reads the saving account balance, my wife's transaction reads the saving account balance and locks it.
- Now my transaction cannot read the saving account balance and my wife's transaction cannot read the checking account balance, so neither transactions can progress.

Deadlock will more likely occur when there are more inter-dependent transactions occurring concurrently. To resolve deadlock, the DBMS will release all the locks but one. As for which lock to leave engaged, the DBMS can use a first-come-first-finish method or the least impact method. Under the least impact method, the DBMS will calculate the optimal system delay (the least) and decide on which locks to cancel. The DBA can choose either method by selecting the respective parameters in the DBMS configuration.

Referential Integrity

Every table must have a primary key in order for each record to be identifiable. A primary key is a field or a combination of contiguous fields in a table that has a unique value from record to record, i.e., the value is never the same between records. Common primary keys are account number and student number. Sometimes, in order to uniquely describe each record, a table has to combine two or more contiguous fields as a composite primary key, e.g., employee_number and client_number can be the primary key in a table that shows the hours worked by each employee for each client. In this case, using either field separately as a primary key does not uniquely identify every record.

Often, the primary key of one table is included in another table as a field other than the primary key. For example, an invoice record should contain a stock ID field. In this case, the stock ID is called the foreign key. A foreign key is a field in a table that satisfies the following conditions:

a. It is not the primary key of the table.
b. It is the primary key of another table.
c. It must not have a null value.

If an invoice does not have a stock ID, it is invalid. This is a good control to avoid billing customers that cannot be traced to goods sold. In this case, the stock ID is the primary key in the inventory table where each record contains information about each stock item.

The DBMS should be configured to check tables for referential integrity, i.e., to check that every record does not have null value for the foreign keys.

Normalization

A normalized table reduces data redundancy by breaking tables to smaller tables, i.e., fewer fields. Tables will be more modular and granular. There are different degrees of normalization. The optimum degree is sixth. A sixth degree normalized table is absolutely free of redundant data. For business applications, third degree normalization is sufficient to avoid the anomalies described above.

A table that is not normalized consists of multiple records pertaining to the same entity and does not have a primary key. For example, if all payroll data is in one table, that would be the case. Keep in mind that a table showing columns and rows is only for

human legibility. In computer storage, a table consists of a long string of 0 and 1. If there are multiple occurrences of the same data fields for an employee in a table without a primary key, the DBMS will have trouble determining where the information for one employee ends and where the next employee shows up in the table. Not only does a long table include redundant data as described above, data access can be inefficient as it takes the DBMS longer to find out where the next record begins by analyzing every data field for every record.

The following is an example of a table that is not normalized.

Table 6.1 - Unnormalized Payroll Table

Emp Num	Pay-per	Pay-date	Last_name	First_name	Dep num	Dep_name	Gross-pay	Netpay
123	1	Jan . 15, 2011	Chan	David	1	Accounting	8,500	5,200
	2	Feb. 15, 2011	Chan	David	1	Accounting	8,500	5,200
456	1	Jan. 15, 2011	Lambie	Shirley	2	IT Security	9,500	5,800
	2	Feb. 15, 2011	Lambie	Shirley	2	IT Security	9,500	5,750
789	1	Jan. 15, 2011	Trivedi	Pat	3	Supply Chain	8,700	5,700
	2	Feb. 15, 2011	Trivedi	Pat	3	Supply Chain	8,800	5,800
790	1	Jan.15, 2011	Williams	Maria	1	Accounting	8,000	5,000
	2	Feb. 15, 2011	Williams	Maria	1	Accounting	8,000	5,100

In the above table, there is no primary key. The field that looks like a primary key is the employee number. However, the record for each occurrence of the employee number has repeated occurrences of the fields in the other values, e.g., the two pay periods, where the name appears twice. This means it is difficult for the DBMS to know how long the record is, or how many instances of repeated occurrences. Keep in mind this is a simple table in terms of the number of rows for ease of reading. Regardless of the length, the DBMS, unlike a person, cannot just read the entire page or pages at a glance, it has to parse every byte. So without a primary key, this table is difficult to understand for the DBMS.

First Degree Normal Form (1NF)- The above table can be converted to first degree normalized by inserting a primary key. The primary key has to be able to uniquely identify every record, i.e., every row. It is easy to see that the key can be composed by combining the emp_num and pay_period fields, to yield the following table. A primary key may contain one field or a group of contiguous fields, in that case, it consists of two fields.

Table 6.2 – First Degree Normalized Payroll Table

Emp Num	**Pay-per**	**Pay-date**	**Last_name**	**First_name**	**Dep num**	**Dep_name**	**Gross-pay**	**Netpay**
123	1	Jan . 15, 2011	Chan	David	1	Accounting	8,500	5,200
123	2	Feb. 15, 2011	Chan	David	1	Accounting	8,500	5,200
456	1	Jan. 15, 2011	Lambie	Shirley	2	IT Security	9,500	5,800
456	2	Feb. 15, 2011	Lambie	Shirley	2	IT Security	9,500	5,750
789	1	Jan. 15, 2011	Trivedi	Pat	3	Supply Chain	8,700	5,700
789	2	Feb. 15, 2011	Trivedi	Pat	3	Supply Chain	8,800	5,800
790	1	Jan.15, 2011	Williams	Maria	1	Accounting	8,000	5,000
790	2	Feb. 15, 2011	Williams	Maria	1	Accounting	8,000	5,100

The primary key is shaded. A first degree normalized table is a table that has a primary key. A first degree normalized table has a drawback in that not every field depends on the entire key. For example, the employee name depends on the employee number but not the pay period number. The employee name therefore appears multiple times between records. This is data redundancy. Such data redundancy can be reduced with further normalization.

Second Degree Norma Form (2NF) – A first degree normalized table can be upgraded to second degree by removing partial dependency, i.e., by making every field fully dependent on the primary key. In the example above, we can break Table 6.2 into the following tables by making every non-key field dependent on the entire key.

In Table 6.2, the first non-key field, pay-date, depends on pay-period but not emp_num. It therefore does not depend on the entire primary key and creates data redundancy, i.e., pay_date values are duplicated across records. This field must be removed from the table and put in another table with pay_period as the key. Last-name, first-name dept_num and dept_name depend on emp-num but not on pay_period. This is why the values for these four fields are repeated between records, we should remove these four fields and put them in a separate table with emp_num as the key.

The remaining fields in Table 6.2 depend on the entire key so they can stay there.

The 2NF tables with limited sample data are shown on the following page.

Table 6.3 – Pay Periods

Pay-period	Pay-date
1	Jan . 15, 2010
2	Feb. 15, 2010

Table 6.4 – Employee

Emp_num	Last_name	First_name	Dept_num	Dept_name
123	Chan	David	1	Accounting
456	Lambie	Shirley	2	IT Security
789	Trivedi	Pat	3	Supply Chain
790	Williams	Maria	1	Accounting

Table 6.5 – Pay Period Details

Emp_Num	Pay-period	Gross-pay	Net_pay
123	1	8,500	5,200
123	2	8,500	5,200
456	1	9,500	5,800
456	2	9,500	5,750
789	1	8,700	5,700
789	2	8,800	5,800
790	1	8,000	5,000
790	2	8,000	5,100

The repeated values in Table 6.5 are attributable to the nature of the data instead of data redundancy. That is, although gross_pay seldom changes from period to period, because it could change and is part of transaction trail, we have to keep track of the data for every period.

Table 6.4 has repeated data, dept_num and dept_name. The repetition of dept_num is natural because there can be more than one employee in a department. However, dept_name does not have to be repeated. What's wrong with repeated data? It means data redundancy. Data redundancy wastes storage, increases lookup time and can lead to data inconsistency, e.g., different dept_names for the same dept_num. Table 6.4 has data redundancy because there is transitive dependency, i.e., dependency between two non-key fields. This redundancy can be fixed by turning any table with transitive dependency into a third degree normalized table by removing the transitive dependencies.
A second degree normalized table is a table that has no partial dependency, i.e., every non-key field depends on the entire primary key.

Third Degree Normal Form (3NF) – A third degree normalized table is a table where every non-key field depends on nothing but the entire primary key, i.e., there is no transitive dependency (dependency between two non-key fields). This degree of normalization is sufficient for business systems to remove data redundancy. The following tables are 3NF. Tables 6.6 is the same as Table 6.3. Table 6.8 is the same as Table 6.5.

Table 6.6 – Pay Periods

Pay-period	Pay-date
1	Jan . 15, 2010
2	Feb. 15, 2010

Table 6.7 – Employee Names

Emp_num	Last_name	First_name	Dept_num
123	Chan	David	1
456	Lambie	Shirley	2
789	Trivedi	Pat	3
790	Williams	Maria	1

Table 6.8 – Pay Period Details

Emp_Num	Pay-period	Gross-pay	Net_pay
123	1	8,500	5,200
123	2	8,500	5,200
456	1	9,500	5,800
456	2	9,500	5,750
789	1	8,700	5,700
789	2	8,800	5,800
790	1	8,000	5,000
790	2	8,000	5,100

Table 6.9 – Department

Dept_num	Dept_name
1	Accounting
2	IT Security
3	Supply Chain

Table 6.4 has been split into tables 6.7 and 6.9.

Summarized Normalization Rules

1. A first degree normalized table has a primary key.

2. A second degree table is a table where every non-key field depends on the entire primary key, i.e., no partial dependency. If the primary key occupies only one field, the table is by default at least second degree normalized.

3. A third degree normalized table is a table where every non-key field depends on nothing but the entire primary key, i.e., no dependency between non-key fields.

MANAGEMENT CHECKLIST

1. Adopt a consistent set of application controls throughout the organization subject to variation between applications because of the nature of transaction processing (e.g., batch vs online) and materiality. For example, there must be monthly reconciliations signed off by managers.

2. Require each system owner to submit a control compliance report annually.

3. Document the internal controls for each business critical system in the same format.

4. Include internal control training as part of new managers' training.

5. Establish a secondment program for people to join the internal audit department for short term assignments and vice versa to increase internal control awareness in the organization.

6. Provide a semi-annual report to the audit committee on overall internal controls reliability in the organization.

7. Ensure that internal control recommendations from auditors are addressed promptly.

8. Include internal control compliance in the performance contracts of executives.

9. Assess the applicability of Six Sigma and initiate a project to achieve it if deemed practical.

10. Include the criteria and measurement of completeness, authorization, accuracy, timeliness and efficiency in each business unit's performance evaluation process.

CONCLUSION

Application controls should be tested on every financial statement audit after testing and gaining assurance on general controls. A moderate level of assurance on general controls and application controls will enable the external auditors to limit substantive testing.

Internal audits mainly focus on internal controls and application controls are usually extensively tested. Other special purpose audits like providing control assurance on a service organization to corporate customers address mainly internal controls including application controls.

Computing power doubles annually. Organizations continue to empower customers and employees with technology by allowing direct access and automated transactions as well as by streamlining manual reviews and approvals. This often leads to removing preventive controls to achieve efficiency. To avoid an unacceptable level of risk, management should design and implement rigorous exception reporting system functions and tracking mechanisms for exceptions to be addressed.

SUMMARY OF MAIN POINTS

- Application controls rest on general controls.
- If general controls are substantially weak, the financial statement auditors may choose to simply walk through application controls instead of detailed testing and adopt a substantive audit approach. Even with a substantive audit approach, auditors place some reliance on internal controls unless the auditors test every transaction. Even if the auditors test every transaction, there is a risk of hidden transactions. So there is always some reliance on internal controls. This is why auditors should at least walk through internal controls. Walkthrough means taking one or two transactions per key control to verify the control. The result of the walkthrough, i.e., presence (with very limited assurance because there is only walkthrough instead of detailed control testing) or absence of controls will influence the auditors in focusing their substantive testing. Even in a substantive audit approach, the extent of substantive testing will differ depending on the result of control walkthrough, e.g., it can range from testing, say 10% of the transactions, to say 50% of the transactions. In other words, a lower detection risk will be tolerated if controls are largely absent as a result of the walkthrough.

- If general controls are reliable, a moderate level of application controls should be sought for the financial statement audit.
- In the audit of a public company in Canada or the United States, the shareholders' auditors are often asked to provide an opinion on internal controls that support the financial statements, in addition to the traditional financial statement audit opinion. In such a case, the shareholders' auditors will seek high control assurance on the internal controls that support financial statements, which means most general controls and most application controls.
- Internal auditors usually seek a high level of assurance and therefore will do more testing.
- Application controls should include an optimum mix of preventive, detective and corrective controls. Preventive controls are preferred, but not all major risks can practically be mitigated with preventive controls, otherwise, the environment may be too tight and therefore not competitive; e.g., it is impractical to require every transaction, regardless of amount, to be pre-approved by management. Hence, detective controls should be put in place to detect significant errors or irregularities and corrective controls are necessary to correct these errors and irregularities.

Common Application Controls

- Edit checks – Applied at input stage, e.g., checking for negative amounts.
- Batch total – Comparing one total accumulated to another total accumulated later in the transaction input phase, to check input completeness. Batch total can also be applied by comparing total input to total output.
- Hash total – Similar to batch total, but the total is applied to a field normally not intended for computation, e.g., check number. This avoids offsetting errors, e.g., a $100 check goes missing but another $100 check recorded as $200.
- Run-to-run control total – Similar to batch total but accumulation and comparison are done by programs within the system, to check the completeness of data passed from one program to another.
- Reconciliation.
- Management review of exceptions.
- Management review of transactions either before or after processing. Some transactions may be impractical or not cost effective for pre-approval, in which case post-approval may mitigate the risk.
- Customer statements.
- Limit check, e.g., checking customer orders to credit limit.
- Monitoring of open items, such as unbilled shipments.

Edit Checks

Edit checks on data input are critical preventive controls to ensure that data input is correct and complete. The same techniques can be applied in processing. Why do we have to apply the same techniques to processing if input data is correct? Well, in processing, programs perform calculations to update data files. Before data files are updated, the calculated results should be validated to detect errors. For example, an invoice with a negative amount should be reviewed before the sales journal and the accounts receivable ledger are updated. Here is a list of common edit checks.

- Check digit to validate data entry of a control number like a product number.
- Data format check, e.g., a date field should be yyyymmdd.
- Limit check.
- Missing data check, i.e., all mandatory fields are filled in.
- Range check.
- Sequence check.
- Sign check.
- Validity check, by verifying data input to a table of acceptable values.

Database Controls

More and more systems use databases. In such a system, there need to be internal controls to ensure data integrity when multiple files (tables) are shared by multiple applications. Here are the common database controls.

- Record locking to avoid concurrent update, i.e., two transactions trying to update the same record concurrently leading to a later transaction nullifying the first transaction.
- Referential integrity to avoid null value for critical fields.
- Detection and resolution of deadlock caused by conflicting record locks to avoid the system being hung.
- Logging of access to database especially changes, to facilitate error recovery.
- Normalization to reduce data redundancy and inconsistency.
- Synchronization between locations and environments to ensure consistency of content and clocks. Clock synchronization is critical to ensure transactions are time stamped correctly for audit trail and for prioritization of updates and interest calculation (e.g., 11:59 pm vs 12:00 am).
- Produce alerts on direct data updates using a non-standard transaction processing system, e.g., updating using a direct SQL command instead of going through a transaction processing system like ATM, to detect unauthorized data change.
- Producing alerts on table creation and deletion to detect unauthorized data creation or change.

REVIEW QUESTIONS

1. What is the difference between redundant data check and referential integrity check?

2. What is the difference between batch total and hash total?

3. Describe an example of what can go wrong if concurrent update is allowed.

4. Describe a technique that can be used as a general control and an application control.

5. Organizations continue to empower employees using information technology to increase efficiency. What is the risk impact and how should management address the impact?

6. Which risk do edit checks mainly address?

7. Give an example of a weakness in general control that will lead to seeking high assurance on application controls.

8. What is the drawback of test data?

9. What is the external auditors' justification for skewing internal control testing towards the first half of the year?

10. What are the similarity and difference between batch total, hash total and run-to-run control total?

CASE – Electronic Order-to-Pay System

A major bank offers an order-to-pay service to its corporate and commercial customers to process their accounts payable and cash disbursements. Customers have found this to increase their efficiency and cash management. This service is web based. Here are the procedures.

1. The bank's corporate customers generate purchase requisitions through their in-house system or the bank's procurement system. The bank's procurement system is used only for generic supplies like computers and office products.
2. The customers' system routes the purchase requisitions to management for approval.
3. The bank's system routes the purchase requisitions to customer management for approval.
4. Management approves online.
5. The bank's system generates purchase orders for review by purchasing agents of the bank.
6. Purchasing agents approve POs online.

7. For purchase orders prepared by customers internally, the customers send them electronically to the bank.
8. The bank's procurement system sends POs to an EDI server.
9. The EDI server computes batch totals and converts POs to EDI format.
10. EDI server sends out POs.
11. Upon inspection of goods, users retrieves the PO from the bank's system and checks the "received" box.
12. System marks the "received" field on the PO table for that PO with a value indicating "received", e.g., 1. Before that, the value may be 0, i.e., not received. This is not the quantity or amount received. It is just an arbitrary value to indicate whether the PO has been receipted or not.
13. Invoices are sent to the bank, but to the attention of customer user organizations by EDI.
14. The bank's accounts payable system matches the PO number on the invoice to the PO file to confirm receipt of goods.
15. If goods have been received, the invoice is scheduled for payment to take advantage of cash discounts and avoid penalty.
16. If goods have not been received, the invoice is recorded in a pending file and the system sends a query to the PO contact for follow-up.
17. Payments are made by EDI.
18. Upon payment, the bank charges the customer and updates the customer's accounts payable ledger.
19. Customers have online access to their POs and accounts payable.

This service is available only to customers to purchase from vendors who agree to invoice and receive payments by EDI.

Required

What internal controls do you expect an organization hosting an order-to-pay system to implement to ensure that transaction processing is authorized, accurate, complete and timely. What controls do you expect a user organization to implement?

RUNNING CASE – Blackberry

What do you think is a business critical system? For that system, analyze the risk using the risk matrix in chapter two. For each cell, describe an application control.

MULTIPLE CHOICE QUESTIONS

1. Which one of the following examples best depicts a preventive control within the expenditure business cycle?

A. The accounts payable manager reviews a list of outstanding accounts payables balances for old or unusual items.
B. The purchasing manager reviews a list of purchase orders issued and follows up on errors noted (e.g., prices, quantities, etc.).
C. The purchasing manager reviews purchase orders for accuracy before the orders are placed.
D. The chief accountant reviews an exception report listing purchase orders issued to vendors not included on the Company's authorized vendor listing.
E. Access control lists for the payroll system.

2. When auditing a retail giant that opens its inventory system to major suppliers for automatic replenishment, which type of controls do you test the most?

A. Input
B. Processing
C. Output
D. Access
E. Data storage

3. Which risk does database normalization reduce?

A. Concurrent update
B. Obsolete data
C. Data redundancy
D. Data incompleteness
E. Data leakage

4. Generally accepted audit standards indicate that shareholders' auditors should try to assess control risk at below maximum. This means:

A. a low range.
B. a high but not maximum level.
C. a minimum level.
D. the median point.
E. a moderate range.

5. What is an auditor's primary concern when reading an organization chart?

A. Clarity of reporting relationship
B. Flattening of organization
C. Extent of distribution
D. Employee names
E. Segregation of duties

6. The mail room sends remittance advices to the accounts receivable department and the checks to the cashier's department. The cashier's department compares checks to deposit slips. With reference to these processes, what control is missing?

A. Bank reconciliation
B. Batch total of the checks and remittance advices
C. Credit limit check
D. Joint signatures
E. Check endorsement

7. Which type of controls is increasingly taking the place of a traditional output control of monitoring the distribution of reports?

A. Input control
B. Edit checks
C. Access control
D. Processing control
E. Management control

8. An employee in the receiving department keyed in an incoming shipment and inadvertently omitted the purchase order number. The most appropriate input control to employ to detect this error is a:

A. batch total.
B. missing data check.
C. sequence check.
D. reasonableness check.

Chapter 7 – Data Analysis Techniques

The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency. – Bill Gates

In Chapter Two, we discussed inherent, control and detection risks. We went through the attributes of IT as they relate to risks. For example, increasing electronic audit trail increases the risk of unauthorized access. Another example is the speed and power of computers, which can decrease the risk of delay. Increasing computing power allows managers to use more data analysis techniques to detect anomalies and irregular practices.

Common data analysis software has the following functions:

- Data import.
- Data export, e.g., exporting analyzed data to Excel for easy graphing.
- Joining files.
- Merging files.
- Data extraction based on criteria (formulae).
- Aging
- Duplicate identification.
- Gap identification.
- Fraud analysis.
- Statistical profiling (analytical review).
- Statistical sampling.
- Regression analysis.

File Import

A data file is necessary in order to use GAS. Common data file (table) formats are text, Excel, dbf. Dbf is a generic database format. Most database tables can easily be saved as dbfs. Most GAS products like ACL can take a data file in just about any format. Data files that are in Excel and dbf can be recognized by a GAS usually automatically without the auditor defining the fields. Text files have to be defined field by field.

File Export

Analyses performed with a GAS tool usually generate new files. One drawback about most GAS products is that they come short in graphical and formatting capability like those in Excel. Often auditors will find it useful to export analyzed files to Excel for more user friendly presentations.

Joining

In the last chapter, we discussed normalization as a control process to reduce data redundancy. This helps to ensure data integrity. However, because normalization creates more tables with fewer fields, sometimes it is necessary to join tables for temporary data correlation, e.g., comparing accounts receivable balance to the credit limit, or comparing the sum of accounts receivable and current order to the credit limit. In auditing, it is also often necessary to compare fields between tables to assess transaction integrity. GAS tools allow a user to join any 2 tables and combine the fields into 1 table as long as the 2 tables have a common primary key.

Extraction

GAS allows you to extract fields from a table into a new table based on any combination of criteria (formulae) defined by the auditor using the drag and drop of standard operands like =, >, <, (,), AND, OR and field names. An example of a criterion is gross_pay > 10000. This is a very useful and versatile function as it allows the auditors to perform tests by means of data correlation and select questionable items for vouching or confirmation etc. Here are some common tests.

- Compare the sum of invoice and account balance to credit limit.
- Select high pay amounts for confirmation.
- Select high receivable amounts for confirmation.
- Obsolescence test by reviewing the date of last sale.
- Cross-reference invoices to receiving reports and purchase orders.
- Compare inventory cost to sale price.
- Check for the system's compliance with inventory costing methods like first-in-first-out, last-in-first-out or average costing by verifying the calculation of cost of sales for selected invoices.
- Look for negative amounts that are usually wrong.
- Verify commission calculation.
- Check for dormant account classification. A bank classifies a deposit account as dormant when there has been no customer initiated transaction for 2 years. Any human initiated transaction like a deposit, withdrawal or transfer made to a dormant account will trigger an alert to the branch manager. An auditor can look at the dates of the last 2 transactions, if the date of the second last transaction is 2 years or more apart from the date of the last transaction, the auditor should flag the account in the audit work papers and then vouch to the management alert that should have been triggered by the last transaction. Dormant accounts are common targets for frauds because the account holders are usually people who do not keep track of the accounts, e.g., senior citizens who live abroad.

Duplicate Identification

Some records should not have duplicate values on certain fields, e.g., the social insurance or social security number. GAS allows auditors to select a field and look for duplicates in the table across records. The output will then be used to present to management for correction.

Gap Detection

This is the opposite of duplicate identification. It looks for gaps. An example of audit test is to detect gaps in purchase order numbers or invoice numbers which should be in sequence.

Fraud Analysis

GAS has statistical analysis functions that can be used to detect fraud. An increasingly used function is called Benford Analysis, based on the Benford Law.

Benford Law

Frank Benford was a physicist in General Electric Company. He enjoyed playing with numbers. In 1938, he stated that in a large series of natural numbers, the probability of the first digit being "1" was higher than that being "2" and the probability of the first digit being "2" was higher than that being "3", etc., and the first digit was least likely to be "9". This theory also applies to the second digit and the successively less significantly leading digits. That is, the probability of the second digit being "1" is higher than it being "2", and the probability of that digit being "2" is higher than that being "3" etc. The less significant the digit, the less it complies with Benford Law. The longer the number (i.e., number of digits in each number) and the larger the population, the more applicable Benford Law is. This theory was also stated by Simon Newcomb, an astronomer, in 1881. However, Newcomb did not perform the extensive research and proof that Benford carried out.

The Benford distribution holds true only for naturally progressing numbers like invoice amount, quantity, age, numerical invoice numbers and check numbers. It does not apply to arbitrarily assigned numbers like social security number, social insurance number and retail sales price. Social insurance numbers and social security numbers are not necessarily sequentially assigned as they were designed to satisfy a check digit algorithm, i.e., not every 9-digit number can be used as a social insurance number or a social security number. Retail sales prices are arbitrarily assigned and retailers often set the prices to start with the digit "9" in order to stay within a low number of digits so customers don't think the products are too expensive.

Benford performed massive numerical analysis to empirically prove this theory and eventually developed a formula to calculate the probability. He derived the following formula for calculating the probability of a number starting with a particular string of digits "n": $Log_{10}(1 + 1/n)$

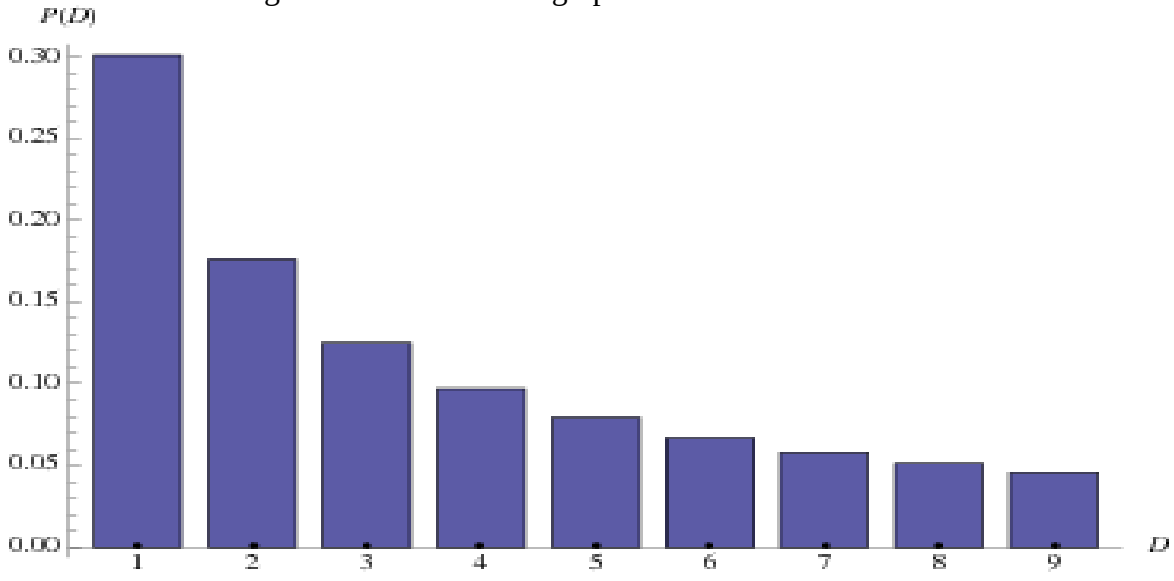
For example, the probability of a number starting with 314 is LOG_{10} (1+ 1/314), or 0.14%. This means, for any number with at least three digits regardless of whether there is a decimal point and where the decimal is, the probability of that number, in the long run, starting with 314 is only 0.14%.

Let's see what the probability of a number starting with 1 is. It would be $LOG_{10}(1 + 1/1)$, or 30.1%. We can calculate the probability of the first digit being 2 to be 17.6% and the probability of the first digit being 9 to be 4.6%.

We can use this formula to calculate the probability of the second digit being 1. For the second digit to be 1, the first digit can be anywhere from 1 to 9. This means we should calculate the probabilities of a number starting with 11, 21, 31, 41, 51, 61, 71, 81, 91 and sum these probabilities. This yields 11.4%. Similarly, we can calculate the probability the second digit being 2 to be 10.9%.

You can see that for the first digit, the probability of a higher order digit (closer to 9) decreases exponentially from 1 to 9. This distribution also applies to the second digit but the slope is less steep.

The Benford first digit distribution can be graphed as follows.



This graph shows the following probabilities of the first digit being 1, 2, 3…..9. This graph can be tabled below.

First Digit	Probability
1	30.1%
2	17.6%
3	12.5%
4	9.7%
5	7.9%
6	6.7%
7	5.8%
8	5.1%
9	4.6%

The probability of the first digit being 0 is not calculated because the first digit will then default to the next digit that is not 0.

Common Sense Reasoning of Benford Law

Most people might think that the probability of a digit being of any value is uniform. For example, in throwing a dice, the probability of each throw is 1/6. However, this thinking does not apply to naturally progressive numbers. When you throw a dice or toss a coin, each throw or toss is not affected by previous or future throws and tosses. However, in a naturally progressive number, the occurrences are inter-dependent. You cannot have two invoices bearing the same number. A 10 year old child will not be 10 years old next year.

Why does "1" have the highest chance as the first digit? Here is a simple example. A child is one year old before turning two. After the age of 9, a child becomes 10 years old and the first digit is "1" again. Then the person becomes 20 years old, etc. Most people won't reach the age of 90. This is an example of why "9" has the lowest chance of being the first digit.

Another example is numerical invoice number. The first invoice would be 1, then 2, and 3…etc. After invoice # 999, it will take 1,001 new sales for the invoice number to have a first digit being "2", and it will take much longer for "9" to claim the first digit again.

Yet another example is the Dow Jones index. It closed today on June 2, 2014 at 16,744. It will take a 19% increase for "2" to claim the first digit. Although a 41% drop will let "9" claim the first digit, it is hard for "9" to keep that title because a 1 % rise will give the first digit back to "1". Benford Law applies to natural numbers, and the numbers do not have to be progressive, they can fluctuate like the Dow Jones index.

Next time you go out of town on the road, place a bet with a companion that the upcoming population signs will have a number starting from 1 to 4. After an 8-hour ride, you may win enough money to treat dinner.

Practical Applications of Benford Law

Benford analysis is useful to assess whether a group of natural numbers representing a particular object includes fictitious items. For example, Internal Revenue Service (IRS) and Canada Revenue Agency (CRA) can use it to review tax returns for overstated expenses like entertainment, maintenance and repairs or for understated business income. Some taxpayers with rental properties might be tempted to overstate repair expenses. Their greed might take them to try to claim $10,000. Psychology tells them that if the amount goes to five digits, it is more alarming or might cross the threshold for tighter scrutiny. So they might report a seemingly random number like $9,276. Well, if a large number of tax returns show repair expense in the $9,000 range or if a taxpayer uses that range or the $8,000 range year after year, the tax department's monitoring system should take note of this and apply tighter audit procedures like asking for supporting documents and authenticating the documents. There are similar applications in corporate fraud detection, consumer fraud detection, as well as analytical review for external and internal audits.

Statistical Profiling

A GAS can calculate statistical parameters like a mean or a median. It can plot numerical distribution, stratification and variance etc. to help an auditor assess the normality of a population of number, e.g., does it fit the normal (bell curve). Many business transaction amounts follow the normal distribution and the Benford distribution. These two statistical distributions have different units of measurement. The normal (bell) curve applies to most natural numbers. For example, extremely low and extremely high invoice amounts would fall at the left and right tails of the curve. It measures the distribution of values. On the other hand, Benford distribution is applied to leading digits regardless of the value of the numbers.

Regression Analysis

This is a useful technique for analytical review. It measures the relationship between a dependent variable and a number of independent variables. For example, if interest revenue is the dependent variable and expressed as x, observations over a period of months can collect enough data to plot the relationship of x = f (y, z). F in this case is the function, and a function can be as simple as a sum or a product of the independent variables. F may be the sum of a constant and a number of independent variables. Y and z in this case are the independent variables. A relationship where there is a constant may be expressing sales people compensation as a relationship with sales, in which case some sales department employees will always get paid regardless of sales. GAS can be useful in plotting relationships. The auditor does not need to know the relationship beforehand. S/he just has to collect a sufficiently large sample of observations of independent variable and dependent variable values. There can be as few as one independent variable. If an independent variable has no bearing on the suspected dependent variable, the coefficient

will be zero or a conspicuously strange value. The auditor should test the derived equation on some specific observations to validate the plotted correlation. A common group of observations is a period of time units or a set of transaction documents like invoices whose values depend on other variables like prices or costs.

Audit Command Language

Audit Command Language is a widely used data analysis software tool. It was developed and is supported by ACL Inc. in Vancouver.

Here is a brief description of how a major financial services company has used ACL.

The company has used ACL to:

- Perform sample valuations on consultant commission fees and compare them to annual sales records to ensure they are accurate and error-free,
- Review client records for cash deposits over $10,000 to comply with reporting mandated by the Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act,
- Develop a list of common suppliers and vendors and the relative expenditures, as part of back-office operations integration. Following this analysis, the company developed a preferred list of suppliers, resulting in overall corporate saving of $600,000.
- Continuously monitor mutual fund trading activity to ensure ongoing compliance with a wide variety of industry regulations, and
- Develop and implement effective fraud detection controls testing which has helped to prevent any problems with fraud or compliance violations within the company

Brief Technical Guide to Using ACL

Here is a brief technical guide in using ACL. The ACL software package comes with a more detailed user guide.

Creating an ACL File

To use ACL, an ACL file must be created. It can be a blank file as a start. This is not a data file, but rather, a file of ACL test documentation including linkage to data files. An ACL file normally includes the ACL analysis work papers for an audit or a section of an audit.

After installing ACL, the user should select File, New to create an ACL file. The file can be named ABCsales. All ACL files carry the suffix of ACL. Now this file is empty. As ACL analyses are carried out, ABCsales.ACL will grow. It is essentially a work paper file of ACL tests.

Importing Data Files

Because ACL is a GAS package, it is useful only when there are data files to be analyzed. ACL can take data files in a variety of formats, including the following common formats, listed in the order of degree of ACL compatibility:

- DBF, database file.
- Excel
- Text with delimiters, i.e., a text file with defined columns.

The PC and LAN versions of ACL have the same capability in accepting data file formats. There is also a Z series server version of ACL. Z series servers store data in the Extended Binary Coded Decimal Interchange Code (EBCDIC) format, whereas personal computers, most mid size computers and LAN servers use American Standard Code for Information Interchange (ASCII). EBCDIC uses 8-bit bytes and ASCII uses 7-bit bytes. EBCDIC therefore allows for more symbols on the keyboard. For example, the letter A is represented using an ASCII byte of 1000001, the EBCDIC representation is 11000001.
A Z series server data file is generally not recognizable to an operating system that uses ASCII. There is therefore a need to use utility programs to convert EBCDIC to ASCII.

When the PC or LAN version of ACL is used to analyse a Z series server data file, the auditors can ask the client or auditee to convert the file to ASCII, in a text file format. It is important that the auditor performs due diligence to ensure the file is genuine and complete. Such due diligence can take the form of being present during the conversion, examining the Z series server's Job Control Language (operating system log), and reconciling the file to ledgers etc.

A data file in DBF or Excel format is immediately recognizable to the PC or LAN version of ACL. A data file in text delimited format can be imported, but the auditor will have to define each field, its format (numeric, alphanumeric, date etc.) and its starting position and length to ACL.

The import of a data file is performed by selecting Data, Select, and identifying the source, i.e., whether it is from a disk or ODBC (Open Database Connectivity, i.e., a LAN where the server is not of the same hardware as the client computer, e.g., a LAN that allows client computers to access a midframe computer like IBM AS 400). In today's environment, the choice of source is most likely a disk. A disk can be a local drive, a portable drive or a network drive. Once the type of source is chosen, ACL will prompt the auditor to identify the file on the drive. ACL will then recognize the file as DBF, Excel or text and ask the auditor to name the data file within ACL. The auditor can use the same file name as the source file. The data file in ACL will be sufficed with .FIL. FIL stands for filter. If the file is not a DBF or Excel file, the auditor will have to define the file layout. ACL will prompt the auditor and guide step by step.

Even if the file is DBF or Excel, the user should check the data type of each field to ensure that a field that will be used for calculation is represented in a numeric form and a field that will be used as a primary key is in alphanumeric form. This can be performed using the following steps:

1. Open the data file.
2. Select, Edit, Input File Definition.
3. Click on the desired field.
4. Check the data type and change it to numeric or ASCII respectively depending on whether the field is needed for calculation or used as a primary key. ASCII is the choice above numeric on the screen. ASCII in this case means alphanumeric.
5. Click the check mark to save.

Extraction

This is the most common function in ACL. It allows an auditor to extract records based on one or more conditions (equations). Here are the procedures.

1. Go to Data, Extract.
2. Click on the If box.
3. Select operands and operators to build equations. An equation can have a number or an input ASCII (alphanumeric) value. The latter has to be enclosed with " ". A date value also can be included in an equation. The format for a date value input by the auditor to an equation is `yyyymmdd` or `yymmdd`, depending the date field that you are trying to compare with, as to whether that field uses a 4-digit year or 2-digit year. A date field, under Input File Definition described above, has the data type of date, not numeric or ASCII. Multiple equations can be combined in an expression by selecting the AND, OR, and NOT operators.
4. Once the expression has been defined, the user should name the output file. If the user wants the output file to be stored in the same folder as the file being analyzed, s/he needs to type in the new file name only. If the user wants the new file to be stored in a different folder, s/he should click on the To box and find the folder.
5. With the Use Output File box checked, the output file will be displayed right away. Otherwise it will stay in the background and the auditor will have to go to Data, Select to find the output file.
6. Now, the user can click the check mark to start the extraction process.
7. At completion of the extraction process, the file history will first be displayed. The file history shows a trail of everything that was done to the file being analyzed. The criteria (expressions) for analysis/extraction, date and time are shown. The user can click on the x mark at the top right corner to close the file history. Then the output file will be displayed. The file history is automatically saved.

Export

ACL is versatile in data analysis but not great in data formatting or graphing. To make up for this shortfall, an analyst can export a file to Excel. This is done by selecting Data, Export and then selecting the type of file format, e.g., Excel.

Join

In data analysis, it is often necessary to join two files so that more fields can be meaningfully compared as a basis of extraction. For example, an invoice file can be joined to an inventory file to check for any sales that are below cost. Two files can be joined as long as they have the same key, even though they have different fields. In fact, the fact that two files have different fields is a common reason for joining the files. The procedures are as follows.

1. With one of the files open, preferably, the primary file, i.e., the file to which another file will be joined, select Data, Join.
2. On the right hand pane, select the secondary file. A file must have been imported to ACL in order to be joined.
3. Select the primary file key and the secondary file key. The two keys must be of equal length; they don't have to have the same name.
4. Select the fields from the primary file and the fields from the secondary file to be joined. Avoid using Select All because ACL will show the fields alphabetically, i.e., the key will likely not be shown as the first (leftmost) field in the output file. You should click the fields, including the key(s) one by one in the order in which you want them appearing in the output file.
5. Unless you want to find out whether any records in the secondary file do not have a corresponding key-match with the primary file, you do not have to select the secondary key as a displayed field in the output file.
6. Make sure you check the box "presort file" for both the primary and the secondary files.
7. If you check the Use Output File box, the output file will be shown right away after the history, otherwise, it will stay in the background.
8. In the To box, name the output file.
9. You can click the If box to perform a conditional join, i.e., combining the Join function with an extraction.
10. The default join criterion is that all secondary records that have a corresponding key match with the primary file will be included. You can expand or change that by clicking the More box and selecting the following:
    - Include all primary records regardless of a match
    - Include all secondary records regardless of a match
    - Include all primary records and all secondary records
    - Include only unmatched records
11. Go back to the Main section and click OK, joining will start.

Analysis Functions

On the main menu, under Analysis, there are a number of functions as follows.

Total – This allows the auditor to total a selected field.

Count – This provides a record count.

Statistics – This calculates statistical parameters like mean, median, standard deviation etc.

Profile – This provides more statistical parameters like min, max and distribution.

Stratify – This provides a summary breakdown based on specified grouping of numerical fields, e.g., # of accounts < $5,000 each, between $5,000 and $10,000, and > $10,000.

Classify – This provides a summary breakdown of different classification, i.e., the field used for classification is alpha-numeric, e.g., # of invoices for each customer ID.

Histogram – This is the graphical format of stratify.

Benford

This function was explained in detail earlier. To exercise it, go to Analyze, Benford, and select the numerical field to be analyzed. Make sure the field represents a natural number. You can select the number of leading digits to analyze, e.g., the first digit, the first 2 digits or the first 3 digits. You cannot select a digit without also selecting the digit(s) to the left. ACL will then calculate the actual numbers of occurrences vs the Benford expected numbers of occurrences and the variances are reported as Z statistics. A Z statistic of 1 or lower is acceptable. Here is an example of analysis result of analyzing only the first leading digit.

Leading Digit	Actual Count	Expected Count	Zstat Ratio
1	23	68	6.428
2	22	40	2.997
3	26	28	0.325
4	25	22	0.607
5	31	18	3.132
6	25	15	2.517
7	24	13	2.981
8	31	11	5.747
9	18	10	2.299

As you can see, the Z statistics for the leading digit being 8 or 9 are quite high. This is inconsistent with the Benford Law that as the leading digit increases towards 9, the probability is lower. From the above analysis, we know that there should be more amounts starting with the digit 1 and 2, and that some amounts starting with the digits 5, 6, 7, 8 and 9 are quite likely doctored. But we don't know which amounts are wrong or fictitious. At least, this leads the auditor to conduct more testing on those ranges of amounts.

Gap

This function enables the auditor to look for gaps in a number sequence. The field to be analyzed can be numeric or alphanumeric, although a gap in an alphanumeric sequence is less meaningful and may not be cause for alarm. The procedures are as follows.

1. Go to Analyze, Gap.
2. Select the field to be analyzed.
3. Click OK.

Duplicate

This function is the converse of gap. The procedures are similar.

Benford Analysis Using Excel

Excel has many numerical functions that are similar to those in ACL, although in a less user friendly manner. An ACL function that can be quite easily performed in Excel is Benford analysis. We will demonstrate it with an example.

Here is a schema of an inventory file.

PARTNOO	Supplier	PART_DESC	VALUE
5416	STEVEN	A248593 HEAT SINK	536500.00
5417	WESTM	730061-12 HINGES	486.00
5431	DRS	A239875 CLAMP VISE	13860.00
5506	FUELMA	BOLT	9.00
5507	FUELMA	CONVECTION PLATE ASSEMBLIES RETURNED	36.00
5520	SNAKES	407-8112-184-16 LH FRAME	632.50
5522	SNAKES	407-8112-183-16 RH FRAME	660.00
5522	MICRO	K1016 W/ KEY WAY	163.20
5530	MICRO	ANGLE & TUBE ASS'Y	1010.10
5538	MICRO	ACTUATING PAWL MOUNT	525.00
5542	WESTM	021907 (10 PCS.)	60.00
5544	STEVEN	A249333 PLAIN QUAD CLAMP	101520.00
5586	WESTM	2806-F REAR RING	3625.00
5587	WESTM	EM105	156.75
5588	WESTM	EM103	151800.00
5589	WESTM	EM103	200.00
5590	WESTM	EM104	165.30
5599	FAM	1/4 X 47MM PIN	30720.00
5603	GEMCO	A401085 R:G NOSE PIECE	1899.80
5605	MICRO	1/2 SHAFTING CUT TO 21 7/8"LONG	126.00
5614	GIEMO	9/16 ROD PIN	899.75
5621	FAM	.312OD TUBING .87 I.D WITH 2 SHOULDER	558.00
5622	GABTEC	HEATSINK #UMD-32/5-3	1140.00
5625	FEMA	ALUM L WITH WINDOW	4080.00
5626	FEMA	ALUM PLATE	9591.00
5627	FEMA	05 SHAFT	910.00
5628	FEMA	05 SHAFT	3825.00
5629	FEMA	HOUSING BLOCK	2625.00
5632	ENGLAN	FP1-5 ARM MODIFIED TO PRINT	750.00
5634	MICRO	05 SHAFT	960.40
5643	FEMA	FEMALE HINGE	230.00
5650	ROY	BLUE TRANSCEIVER LENS	1419.00
5654	MICRO	HEAD BEARING	154.00
5655	STEMCO	011-500-6 (4 SETS)	300.00
5656	STEMCO	000-503-6 .062 THK STEEL (16PCS)	200.00
5658		CUTTING O.P.P. SQUARE TUBING	16800.00
5659	STEVEN	C'BORE QUAD CLAMP #A246914/SS5	420.00
5660	FEMA	LOCK ROD	170.00
5661	FEMA	DRIVE SPINDLE	475.00
5663	PEASAN	ALUM. PCS.	2212.00
5667	PEASAN	BLOCKS	4225.00
5667	HSMETA	#68A CASTINGS MACHINED	1603.24
5669	HSMETA	#68 CASTINGS MACHINED	1078.76
5670	MICRO	ALUM SHAFTS	100.00

An analyst can take the following steps to use Excel to perform a Benford analysis.

1. Set up a table of Benford distribution based on an earlier section of this chapter that describes the Benford Law, as follows.

   Benford First Digit Distribution

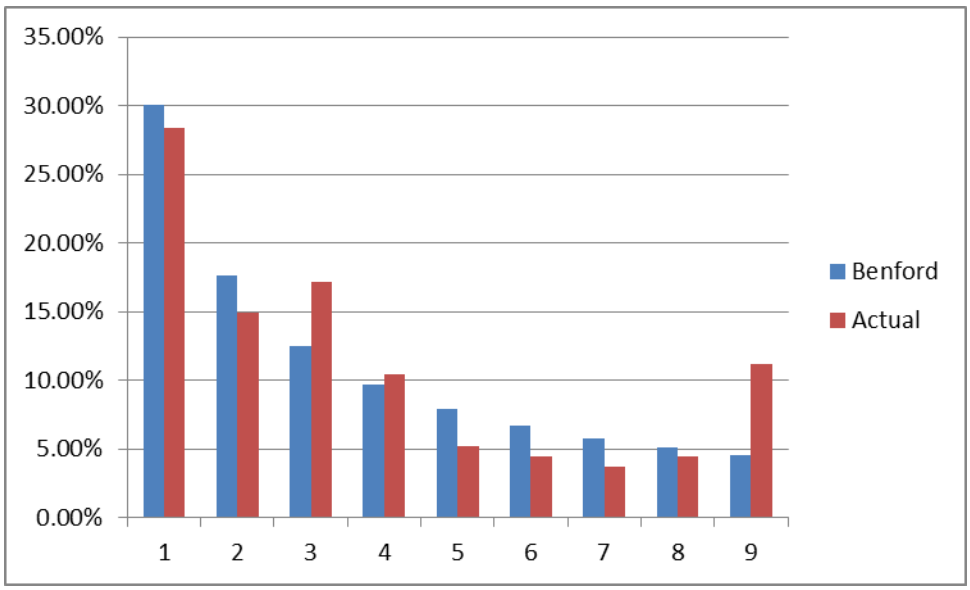
1	30.10%
2	17.60%
3	12.50%
4	9.70%
5	7.90%
6	6.70%
7	5.80%
8	5.10%
9	4.60%

2. On a new column, collect the first digit of the inventory values with the LEFT function.

3. Count the number of occurrences of the first digit of inventory values being "1, "2", …."9", with countif function, =countif(range of the first digit row in the first digit column prepared in step 2, the first column of the Benford Distribution table above).

4. Create a column that is the product of the second column of the above Benford table and the total number of rows of inventory parts in the inventory table. This column therefore represents the number of inventory parts whose values are expected to start with 1, 2,…9 etc.

5. Plot a column chart that compares the results of steps 3 and 4. The chart is displayed on next page.



CASE – Loan Approval

Study the following system description.

Check data completeness and perform edit checks.
If gross income > $50,000, ask about consumer loan and credit card payments, else send application for management review.
If consumer loan and credit card payments < 10% of gross income, ask about mortgage payments, else send application for management review.
If mortgage payments > 20% of gross income, exit and send application for management review.
Ask about years employed.
If years > 4, grant $10,000 limit, else grant limit = $10,000/4 x number of years employed.

Required

Discuss in detail how you would use ACL to test this system.

CHAPTER EIGHT – COMMON ACCESS CONTROLS

If you know the enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory you will suffer a defeat. If you know neither, you are doomed. - Sun Tzu, *The Art of War*

Home Depot Security Breach in 2014

Home Depot's in-store payment system wasn't set up to encrypt customers' credit- and debit-card data, a gap in its defenses that gave potential hackers a wider window to exploit, according to interviews with former members of the retailer's security team.

It's unclear whether that vulnerability contributed to the hack that Home Depot announced on September 8. Yet five former staffers describe a work environment in which employee turnover, outdated software, and a stated preference for "C-level security" (as opposed to A-level or B-level) hampered the team's effectiveness. The former workers, including three managers, asked that their names not be used because they fear retribution from their former employer; some now work for companies that perform security functions for Home Depot.

Although the company this year purchased a tool that would encrypt customer-payment data at the cash register, two of the former managers say current Home Depot staffers have told them that the installation isn't complete.

"We're continually working to enhance our IT security to protect customer data, and we've taken aggressive steps to address the malware in this breach," says a Home Depot spokeswoman. "It wouldn't be appropriate for us to comment on such rumors and speculation in the midst of our investigation."

A "health check" on Home Depot's information systems, which was performed two months ago, identified out-of-date malware-detection systems, according to a former manager. Hackers may by then have been rifling through the company's computer data. Home Depot has said that the hack may have begun as early as April and has the potential to compromise customers who used credit cards or debit cards at 2,155 stores in the U.S. and Canada.

The former information security managers say that when they attempted to make improvements to Home Depot's security systems, they were at times turned down by its technology executives. Two former managers, who left the company in 2011 and in 2012, said an IT executive told them to settle for "C-level security" because ambitious upgrades would be costly and might disrupt the operation of critical business systems. This management style frustrated a number of workers in Home Depot's information security department, leading to dozens of departures from a team of fewer than 50 over the past three years, according to the former managers.

High turnover in information security departments can be costly because of the training that's required for such positions, says Anup Ghosh, chief executive officer of Invincea, a security company in Fairfax, Virginia. "Every time you have turnover, you're training the next person and losing the institutional knowledge of people there," Ghosh says.

The former managers say they were troubled by the lack of encryption for credit-card data at Home Depot stores. Data were sent from the stores to central servers in clear text, according to two of the former managers. This year, they say, Home Depot purchased a tool to encrypt the card data, but the system had not been implemented.

Three former information security managers also say that Home Depot was using out-of-date antivirus software for its point-of-sales systems.

Source: Bloomberg, September 12, 2014.

JPMorgan Hack in 2014

The biggest U.S. bank, said a previously disclosed data breach affected 76 million households and 7 million small businesses. Customer names, addresses, phone numbers and e-mail addresses were taken, the New York-based bank said today in a regulatory filing. Hackers also obtained internal data identifying customers by category, such as whether they are clients of the private-bank, mortgage, auto or credit-card divisions, said a person briefed on the matter.

The breach affected anyone who visited the company's websites, including Chase.com, or used its mobile app, said the person, who requested anonymity because that information wasn't publicly disclosed. Some of those affected by the incursion are former clients of JPMorgan, which currently has 65 million customers and reaches half of all U.S. households, the person said.

"There is no evidence that account information for such affected customers -– account numbers, passwords, user IDs, dates of birth or Social Security numbers –- was compromised during this attack," the company said.

The number of households affected by the attack on JPMorgan compares with the 145 million personal records taken earlier this year in a breach of EBay Inc. and last year's attack on retailer Target Corp., which affected 110 million.

The attack, which is being probed by FBI, started in June at the digital equivalent of the company's front door, exploiting an overlooked flaw in one of its websites, two people familiar with the bank's investigation have said. The hackers unleashed malicious programs designed to penetrate the corporate network, the people said. With

sophisticated tools, the intruders reached deep into the bank's infrastructure, siphoning gigabytes of information, until mid-August. Only then did a JPMorgan team conducting a routine scan trigger an alarm. They discovered a breach that investigators believe originated in Russia, the people said.

Government officials and security specialists have long warned of the possibility of cyber disruptions in the financial system and other essential services and utilities. Those concerns are heightened in times of conflict.

Russia's annexation of the Crimean peninsula touched off a wave of sanctions in March that have hurt trade and threaten to send President Vladimir Putin's economy into recession. Tensions mounted as the conflict expanded beyond Crimea and as the U.S. and Europe deepened their protests of Russia's actions. Dmitry Peskov, a spokesman for Putin, dismissed the notion that Russia was behind the JPMorgan attack as "nonsense."

Source: Bloomberg, October 2, 2014

Iran Nuclear Meeting Hack

Further research into the sophisticated computer virus used to hack into hotels where the Iran nuclear talks took place has found it took advantage of digital credentials stolen from the world's top contract electronics maker Foxconn.

Russian security company Kaspersky Lab said on June 15, 2015 that researchers learned the Duqu 2.0 virus had redirected computer traffic by using a legitimate digital certificate from Taiwan's Hon Hai, also known as Foxconn.

Foxconn customers have included many of the world's biggest electronic makers, including Apple, Blackberry, Google, Huawei and Microsoft.

Kaspersky revealed its initial findings in a report last week in which it said it found the virus in conferencing equipment at three European hotels used in talks involving Iran and six world powers, among other targets.

Digital certificates are the credentials which identify legitimate computers on a network. They act as the basis of e-commerce and other largely automated transactions on the Web.

In recent years, cyberspies have begun to exploit stolen certificates to trick machines into thinking malicious software comes from legitimate computers, an escalation posing a grave threat to business done over the Internet, security experts say.

The "P5+1" group of six world powers have been negotiating with Iran on curbs to its disputed nuclear programme - the United States, Russia, China, Britain, France and Germany.

The on-again, off-again series of talks to reach a comprehensive nuclear deal with Iran have been held in Geneva, Lausanne, Montreux, Munich and Vienna since last year.

Both Moscow-based Kaspersky and U.S. security company Symantec Corp said the virus shared some programming with previously discovered espionage software called Duqu, which security experts believe to have been developed by Israelis.

Israel, which has strongly opposed the powers' diplomatic opening to its arch-enemy Iran, denied any connection with the virus. In February, the United States accused Israel of using selective leaks from the talks to distort the U.S. position.

The West suspects Iran wants to develop a nuclear weapons capability from its enrichment of uranium. Iran says it wants nuclear energy only for electricity and medical isotopes.

Symantec and Kaspersky analysts have said there was overlap between Duqu and Stuxnet, a U.S.-Israeli project that sabotaged Iran's nuclear programme in 2009-10 by destroying a thousand or more centrifuges that were enriching uranium.

The Stuxnet virus took advantage of stolen digital certificates from two other major Taiwanese companies, JMicron Technology Corp and Realtek Semiconductor Corp , Kaspersky said in a report it published in 2010.

"Duqu attackers are the only ones who have access to these certificates, which strengthens the theory they hacked the hardware manufacturers in order to get these certificates," Kaspersky said in a summary of its report on Monday.

Kaspersky said it had notified Foxconn of the stolen credentials. Foxconn was not immediately available to comment on steps it has taken to secure its systems.

Last week, Kaspersky said Duqu 2.0 had evolved from the earlier Duqu, which had been deployed against unidentified targets for years before it was discovered in 2011.

It said Duqu 2.0 used three previously unknown flaws in Microsoft Corp software to infect machines, for which the software giant subsequently released patches to fix. The attack left almost no traces. (Reporting by Eric Auchard in Frankfurt and Joseph Menn in San Francisco; Editing by Mark Heinrich)

Source: Reuters, June 15, 2015

Management must link access controls to business strategy and realize that the main purpose of security is to enable business growth and success. The chief information security officer must structure and advertise the information security program for it not to be seen as an inhibitor. Security measures are like brakes. They allow a car to go faster as without deficient brakes, one would hesitate to accelerate. In developing the information security strategy to be congruent with the business strategy, the principle of least privilege should generally be applied, i.e., one should be given enough information to perform the job. However, this principle does not conflict with the principle of empowering employees and customers. Non-sensitive information should be widely available to employees and customers, e.g., the organization chart of every department

can be available to every employee so s/he will understand the business and organization better and do more networking; company products and locations can be made available to customers to increase their interest and sense of attachment to the company.

Management must realize that security is a form of internal controls and there the organization should implement security to provide reasonable, but not absolute assurance. This means the information security program must be cost justified, as opposed to "security at all cost." The cost justification, of course, should also take into account the intangible risk of reputation damage, loss of customer goodwill and morale degradation etc.

In Chapter Two, we discussed the risk factors related to completeness, authorization, accuracy, timeliness, occurrence and efficiency. We also reviewed some examples of what have gone wrong with information systems. One type of mishaps particularly related to authorization is security breach. Here is a common list.

- Hacking
- Hardware theft
- Identity theft
- Inappropriate use of IT resources
- Internal breach
- Sniffing
- Software theft
- Spoofing
- Virus
- Worm

To mitigate these risks, an organization must implement preventive and detective access controls tailored to the environment. These controls can take the forms of software, instructions, procedures and physical devices.

Hacking

Every computer is hackable to some extent, unless it is turned off. This is a smokeless crime and the identity and source of hackers are often concealed. Here is a list of common payloads:

- Obtain system information to perform further crime like identity theft.
- Obtain sensitive customer or business information to achieve malice like blackmail or to embarrass people.
- Obtain sensitive information just for curiosity. The risk is that the suffering organization has no control as to how the hacker uses the information.

- Deface a web site.
- Change a web site's information, e.g., changing a customer agreement to make the organization liable for something which the organization has disclaimed in the agreement, or changing an advertised price or interest rate.
- Bring down or jam a web site.

A hacker can install a rootkit in a computer after first obtaining root-level access, either by exploiting a known vulnerability or by obtaining a password using password cracking or social engineering. Once a rootkit is installed, it allows a hacker to mask the ongoing intrusion and maintain privileged access to the computer by circumventing normal authentication and access controls. Rootkits are commonly used in setting up and hiding malicious software, or injecting malicious software in otherwise normal programs.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include file integrity monitoring and intrusion detection systems. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. The kernel is the core of an operating system that directly controls the allocation of the central processing unit (CPU) functions and random access memory (RAM). The CPU is the core hardware of a computer that performs simple calculation and data comparison without the aid of software.

Another common hacking technique is to inject SQL code in an Internet transaction session. This means a hacker will key in some SQL code (program instructions) in fields that ask for data input to process a transaction like a Web order. A successful SQL injection may allow an attacker to spoof identity, collect information, and tamper with or destroy existing data. Spoofing means hiding one's identity by using another identifier to pretend to be the owner of that identifier, e.g., using someone else's IP address in place of the hacker's to hide the hacker's traceability. Here is an example of SQL injection.

Consider a web application that allows users to change their passwords and asks for following inputs:

UserID: 'chand'
Old password: Soccer99
New password: Potash9999
The resulting SQL executed by the database then is:

```
UPDATE usertable SET pwd='Potash9999' WHERE
        userid='chand';
```

This changes the pwd value in the user table for the user 'chand'.

Now, if the user provides the following special input instead:
UserID: 'chand' OR userid = 'admin'
Old password: Soccer99
New password: Potash9999

The resulting SQL executed by the database then is:

```
UPDATE usertable SET pwd='Potash9999' WHERE
    userid='chand' OR userid = 'admin'
```

This changes the password of the user 'admin', a commonly used ID for system administrators.

Hacking can be prevented and detected using a combination of access controls like firewall, strong passwords, intrusion detection system, intrusion prevention system, security training to programmers to be able to code instructions to prevent SQL injection, vulnerability assessment, penetration testing (ethical hacking), rigorous testing of programs, inclusion of security practices in programming standards, and encryption. We will discuss these controls later.

Hackers are increasingly financially motivated to obtain business and personal information to commit fraud. For example. In April 2014, many governments and large organizations including financial institutions became alarmed about the Heartbleed vulnerability which can be used to obtain supposedly encrypted information passed through the Internet as part of trusted eBusiness. This led to Canada Revenue Agency (CRA) shutting down its web site for eFiling for five days. When the site was reopened, CRA said the social insurance numbers of about 900 taxpayers had been stolen from the site in connection with Heartbleed. The alleged 19 year old Stephen Solis-Reyes of London, Ontario, was arrested by Royal Canadian Mounted Police on April 16, 2014.

Heartbleed

The Heartbleed Bug is a serious vulnerability in the OpenSSL cryptographic software library. OpenSSL is the open source code for Secure Socket Layer, the cryptography protocol for eBusiness. This weakness allows stealing the information protected, under normal conditions, by SSL/TLS encryption. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

This bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. The intruder does not need any privileged credential. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. It allows attackers to eavesdrop on communications and steal data directly from the services and users. A fix has been released by Openssl.org.

This bug is in the OpenSSL's implementation of the TLS/DTLS (transport layer security protocols) heartbeat extension. The heartbeat extension is a piece of program code that lets a client test whether the connection is live before passing information. This is why the bug is called Heartbleed. When it is exploited it leads to the leak of memory content from the server to the client and vice versa. An intruder can repeatedly obtain chunks of 64 kilobytes of data including the private key on web servers and the symmetric key generated by clients. If the private key is obtained, an intruder can derive the SSL key

used in eBusiness and thereby decrypt financial and other sensitive information that has been encrypted before transmission. The intruder can also play person-in-the-middle attack by disguising as a secure eBusiness web site.

The most notable software using OpenSSL are the open source web servers like Apache and nginx. The combined market share of just those two out of the active sites on the Internet was over 66%, according to Netcraft's April 2014 Web Server Survey. Fortunately many large consumer sites are saved by their conservative choice of SSL/TLS termination equipment and software, i.e., not using open source like OpenSSL.

This bug was independently discovered by a team of security engineers (Riku, Antti and Matti) at Codenomicon, a Finnish security firm and Neel Mehta of Google Security, who first reported it to the OpenSSL team. Codenomicon team found Heartbleed bug while improving the SafeGuard feature in Codenomicon's Defensics security testing tools and reported this bug to the National Cyber Security Center Finland (NCSC-FI) for vulnerability coordination and reporting to OpenSSL team.

Immediately after the discovery on 3rd of April 2014, NCSC-FI took up the task of verifying it, analyzing it further and reaching out to the authors of OpenSSL, software, operating system and appliance vendors, which were potentially affected.

Google, Microsoft, Twitter, Facebook, Dropbox, and Amazon remained safe, but Yahoo.com was vulnerable. Within a day, Yahoo said it had successfully patched the bug on its homepage, search, mail, finance, sports, food, tech, Flickr photo and Tumblr blogging services. Canadian banks have indicated that they are protected from this bug. Rumours have it that the United States National Security Agency (NSA) had known about this vulnerability for two years, but this was denied by NSA.

Bugs like this one will keep surfacing. Rigorous software testing before release and relentless network monitoring are standard practices in large organizations. Security professionals and systems developers must try their best…and hope for the best.

Hardware Theft

As computing devices become smaller, they are subject to a higher risk of theft. The loss of hardware often also means the loss or disclosure of information. Organizations should provide users with notebook computer locks. It should educate users about the risk of theft and preventive measures. Networks should enforce passwords and encryption to minimize damage in case a device is stolen. Accurate inventory can aid in disabling the network access capability of lost devices.

Inappropriate Use of IT Resources

Today’s employees are highly empowered in terms of IT tools. Most office employees have Internet, email, PCs, network folders and office productivity software. These tools help to commit wrongdoing, e.g., using the tools for non-work purposes to a significant extent or using the software to break the law, violate organizational policies, harass or in

a way that will expose the organization to bad reputation or legal liability. It is critical for organizations to state clearly what uses are not acceptable. Research studies have shown that as much as half of Internet traffic in a typical blue chip corporation is not for work purpose.

Why is this a security concern? Excessive use of IT resources for non-work purposes could affect system availability. Installation of unlicensed software can expose the organization to legal liability and introduce viruses or worms. Access to indecent web sites like child pornography or terrorist sites can incriminate an organization.

Identity Theft

Increasing personal information is stored electronically that can be accessed via a network. This is why criminals are more and more interested in stealing identities to enter into contracts, make purchases or cross borders using the stolen identities. The increasing number of social media sites escalates this risk.

Identity theft may be achieved using a combination of malicious acts including hacking, shoulder surfing and social engineering. Social engineering means someone posing as a legitimate party asking for seemingly benign information and then step by step gaining security intelligence about the organization and the intelligence will then be used to aid in identity theft. For example, a visitor to a major high tech company was able to enter an open office area on a Friday afternoon where documents, unlocked notebooks and memory sticks were lying on desks and some on the floor. The visitor politely asked to go to the washroom when sitting in the waiting area of the company. The security guard let the visitor in without calling the person who was being visited. After coming out of the washroom, the visitor followed employees into the office area. In this case, social engineering was achieved because employees were not well trained to follow procedures and challenge strangers. A common instruction to employees is to never hold the door open for anyone they don't know or anyone they know should not have access to the area behind the door.

An increasingly common method in identity theft is phishing. This means sending email to people to entice them to release their personal information or to entice them to access a hacker site that can tap their personal information. Here is an example.

RBC Royal Bank Customer,

Your account was recently accessed from a location we're not familiar with. Please review the activity details below:

Location: Germany
Time: Today at 12:10am EST
Location estimated based on IP=87.118.101.175
"That was me." **"That was NOT me."**

If anything looks unfamiliar, RBC will help you secure your account to prevent people in the future from accessing your account without permission.

Royal Bank Online Security

I knew this was not from Royal Bank. First, the name of Royal Bank in Canada is RBC Financial Services. Secondly, I know banks don't send unsolicited email to customers to ask them to perform a function by clicking an embedded link in the email. Thirdly, the signature line just says Royal Bank Online Security, which is too brief to be business like. Fourthly, the two links provided do not point to Royal Bank web sites.

Organizations should educate their employees and customers about phishing, i.e., do not click on links embedded in emails that they don't expect or recognize and do not respond to such emails. A phish is an email purporting to be from a legitimate organization asking for identity or account information as part of social engineering.

Internal Breach

A 2008 FBI survey indicated that 25% of security breaches occurred within organizations. This is probably a conservative number because organizations tend to report external intrusion more than internal breaches. Insiders have an edge because they don't have to beat the firewall and they know the people, the organization's culture and systems.

It was reported in New York City media in September 2010 that a software engineer of an IT giant company used his internal clearance to access user accounts, including the information of four minors. This is just one of many types of breaches. Other common breaches include internal hacking, password cracking and copying information from an unattended computer.

Spam

The extent of junk mail is not just a nuisance. It is a security threat. Employees may receive so many spam messages that they may not read carefully before clicking on a link or opening an attachment, therefore getting infected with a virus or allowing a hacker to install a malicious program. Employees may also give out sensitive information. Some employees may delete work related messages because they think the messages are spams. Organizations should take measures such as installing a spam filter program to keep spams out.

Canadian Anti-spam: Legislation comes into effect on July 1, 2014. This new law will prohibit the: (a) Sending of commercial electronic messages without the recipient's consent (permission), including messages to email addresses and social networking accounts, and text messages sent to a cell phone; (b) Alteration of transmission data in an electronic message, which results in the message being delivered to a different

destination without express consent (a process common in phishing scams); (c) Installation of computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee; (d) Use of false or misleading representations online in the promotion of products or services; (e) Collection of personal information through accessing a computer system in violation of federal law (e.g. the *Criminal Code of Canada*); and (f) Collection of electronic addresses by the use of computer programs or the use of such addresses, without permission (address harvesting). This new law will impact everyone. Individuals, incorporated and unincorporated businesses and not-for-profit organizations need to review how they are sending electronic messages for commercial purposes. *Source:* http://fightspam.gc.ca.

Sniffing

One way to gain unauthorized access to information is to sniff it in transmission. This can be done using one of the following common methods:

- Installing a sniffing program on a networked computer.
- Connecting a sniffing device to a router or switch.
- Connecting a sniffing device to a circuit.
- Connecting a computer with a sniffing program or a sniffing device to a wireless channel.

The sniffed data will then be analyzed and deciphered to achieve the goal of gaining unauthorized access to information. Wireless networks are more vulnerable.

Software Theft

Software theft is harder to prevent and detect because it is less visible. Software theft can lead to legal liability if the licensed software is used by unauthorized parties. It can also lead to loss of competitiveness; imagine a software giant having the source code of its flagship product exposed! Software theft can be prevented with access controls, employee education and stringent procedures covering software update, storage and distribution.

Spoofing

This means obtaining access using false identity. It is not the same as identity theft as spoofing does not really use the stolen identity to commit a crime or obtain financial gain. Spoofing is used by hackers to hide the source of hacking. It can also be used by someone to send email under a pretended email address. For example, John Doe could send email as Mary Amato without actually using Mary's email address. A simple way is for John to change the displayed name of the sending email address to Mary Amato.

Spoofing is also used by hackers to hide their IP addresses to fool firewalls and make it difficult for the police to track them down. Rigorous firewalls and intrusion detection systems can serve to mitigate this risk.

A hacker can also spoof the media access control address to beat any MAC address filtering by routers and to implicate someone else. Strong encryption for wireless networks, rigorous firewall configuration as well as hardened work station and server operating systems parameters can serve to mitigate this risk. Hardening means disabling unnecessary functions (operating system services) of the operating systems to lessen exposure to hacking and also installing the latest security fixes from vendors.

Organizations can prevent email spoofing using advanced email checking techniques like digital signatures and adopting sophisticated firewall rules. User education would also help.

Virus

This is a common threat. A virus is a program on its own or is attached to a legitimate program. A virus can be contracted when the program is triggered, unless the object exposed to the virus is equipped with the proper anti-virus software. Common channels of contamination are email attachments, downloading programs and program sharing. A Word, Excel or Powerpoint macro is a program so it can be virus borne. A virus may be a malicious program on its own or it may be a useful program that also contains malicious code, in which case it is called a Trojan. Here are the common payloads.

- Erase an operating system file causing the computer to misbehave or shut down.
- Copy or erase a password.
- Try to logon to a system using a user ID and guess the password, thereby locking out the user because of unsuccessful password attempts.
- Erase data.
- Log key strokes and send them to a hacker site.
- Copy sensitive data and send it to a hacker site.
- Plant a logic bomb to act up based on certain conditions or on a certain date to cause the above damage.
- Pick an email address from the infected computer's address list to send a strange email along with a copy of the virus to other addresses on the address list, thus causing confusion or panic and spreading the virus.
- Disable the operating system's security settings.
- Erase memory in the boot sector. The boot sector is reserved memory in a hard disk or USB that interfaces with the computer's Basic Input Output System (BIOS) to boot the computer. It typically is used to store the start up operating system commands.

A virus spreads mainly by sending a copy of itself by email. The common ways of getting infected are:

- Clicking on an email attachment or a URL that contains the virus.
- Opening a file that contains the virus.

A virus is an equal opportunity damage agent. It usually does not differentiate between types of organizations or applications. It is usually operating system specific. Thus, a virus is seldom capable of changing or deleting specific financial files; although it could erase the entire hard drive. A virus can attack a system vulnerability or simply use the standard operating system services of a healthy system. The former can do more damage.

Common solutions are to use frequently (daily) updated anti-virus software, user education about avoiding strange email and blocking program files that come in as email attachments.

A computer virus is actually equivalent to a bacterium rather than a biological virus. It requires a subject's action to spread, i.e., to click on the virus or virus borne program file. There is a specific cure for it; anti-virus software is analogous to anti-biotic, although the former is preventive and the latter corrective.

Vulnerability

In information security, a vulnerability is usually present when too many operating system services are activated or configured to be launchable. A service is an operating system program that performs repetitive functions, it is a system program, as opposed to an application like Word or Excel. Some services are not required by most users so should be disabled. Organizations should assign computers to users with minimal services enabled. A vulnerability may also be present when a hacker has written an exploit to combine some individually benign services to launch an attack. In this case, the operating system vendor will publish the vulnerability and the patch and if the latter is not available, the vendor should still publish the vulnerability and provide procedures to help users to avoid the vulnerability being attacked on.

Worm

This is similar to a virus, but is more stubborn and it spreads faster. It is more difficult to address than a virus. To help understand its resilience, one could equate it to a biological virus. A biological virus is easier to contract than bacteria as it is smaller and lighter so can travel more in the air and one can contract it just by being sneezed on or by touching a door handle and later touching the lip.

A worm travels on a network and can infect any computer that is on the same network. When a computer is on the Internet, it is widely exposed to worms. However, just like virus infection of a human body, a healthy computer is less susceptible to viruses or bacteria infection. A perfectly healthy computer is immune to worms. What does this mean?

Once a worm enters a computer, it looks for the vulnerability that the worm was written to exploit. A common type of vulnerability is a security hole in a system software product like the operating system that opens a back door to worms and hackers. If the

vulnerability is found, the worm will release its payload which commonly generates a high volume of meaningless but resilient packets to clog up the computer and the network. It could also disable anti-virus software and other security measures. A worm may be memory resident only or may stay on your hard disk. The high volume of packets will achieve denial of service. Imagine someone programming a computer to call your phone continuously!

A common technique used in worms is the SYN flood attack. This occurs when a computer sends a flood of TCP/SYN packets, often with a forged sender addresses. Each of these packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (acknowledge), and waiting for a packet in response from the sender address (response to the ACK packet). Normally when a client attempts to start a TCP connection to a server, they exchange a series of standard introduction messages which normally runs like this:

1. The client requests a connection by sending a SYN (synchronize) message to the server.
2. The server acknowledges this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol. A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it knows that it did not send the SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

A worm may also be programmed to launch a distributed denial of service scheme by using each infected computer as a zombie to carry out SYB flood attacks, hence disabling a network within a short time.

A worm can also disable security features like anti-virus software or password checking (which may lead to access allowed without authentication). A worm may also delete files. Generally, a worm will inherit the access right of the user who is currently logged on.

Worms are written to exploit system vulnerabilities. When the hacker community publishes a vulnerability in, say, a commercial operating system, hackers will get on to write and propagate a worm to exploit the vulnerability. Zero day exploits, i.e., worms that are written within a day from the publicizing of vulnerabilities, are increasingly common. This leaves little time for the software vendor to develop and distribute fixes (patches). It is therefore important for organizations and users to understand that it is not enough to just rely on patches; rather, operating systems, browsers and other system

software tools should be configured to activate only the "services", ports and system functions that are needed for the user's and organization's operation. This practice is somewhat analogous to leading a healthy life style instead of taking a lot of vitamin pills. Common solutions to worms are to patch (update) system software and to reinstall anti-virus software. Anti-virus software can only remove worms from the hard disk. To prevent reinfection, the computer must be patched with the latest fix that closes the security hole that the worm is exploiting.

ACCESS CONTROLS

In Chapter Three, we talked about general controls as internal controls that are applied to a multitude of systems. General controls should be implemented as the foundation on which application controls will sit. One of the major types of general controls is access control. Access controls can also be implemented at an application level. Some access control tools can be deployed at a general level and an application level, e.g., passwords. Access controls are also called security. In this chapter, we will discuss access controls that are commonly used in an organization, whether they are applied at a general or application level.

Access controls mitigate the risk of unauthorized transactions, unauthorized change to information and unauthorized viewing of information. They also support software change control and segregation of duties, e.g., by prohibiting a programmer from implementing programs without testing. Access controls also support application controls by, e.g., preventing unauthorized change to electronic bank statements that would compromise bank reconciliations.

There are three objectives in implementing access controls. They are integrity, confidentiality and availability. Integrity calls for access controls to prevent and detect unauthorized change. Confidentiality means no unauthorized viewing. Availability assurance will require access controls to mitigate the risk of system outage. You might wonder why we talk about availability here, since the controls against system outage are discussed in Chapter Three under disaster recovery planning and backup. The link between security and availability mainly has to do with hackers and viruses. These two malicious agents often cause computers to lose their functions.
How are these three objectives related to the control criteria of completeness, accuracy, authorization, timeliness and occurrence? These five criteria are affected by access controls that ensure integrity and availability. A system without integrity will most likely produce inaccurate information. A system that is not consistently available will lead to untimely processing. A system that has no access controls will be vulnerable to a lot of unauthorized transactions.

Why don't we just use the five control criteria above as a frame of reference to discuss access controls, instead of focusing on confidentiality, integrity and availability? First, the six control criteria do not directly address confidentiality and availability. Secondly, access controls address mainly authorization and occurrence and have less direct impact on completeness, accuracy, timeliness and efficiency.

The three access control criteria are confidentiality, integrity and availability. Further, every access control will perform one of the following five functions:

- Identification
- Authentication
- Authorization
- Logging
- Monitoring

Each process may address multiple objectives and the extent to which each objective is met depends on the access control that falls into a process. Let's use a common system, automated teller machine (ATM), to demonstrate these five processes.

1. You insert your card to be identified.
2. Your personal identification number (PIN) is used to authenticate you.
3. Your daily withdrawal limit is used for authorization.
4. Your transaction is logged.
5. Try to use your card at ten locations on the same day, guess who will leave you a voice mail message before the end of the day….that's monitoring.

In the rest of this chapter, we will discuss the common access controls, i.e., access control techniques that can be applied at a general level and an application level. These controls are common to many operating environments and applications. Access controls may be manual, procedural, physical or logical. A manual access control involves mainly human review or authorization. A procedural access control involves mainly policies, standards or procedures. A logical access control relies mainly on software, e.g., a password.
A physical access control relies mainly on hardware, e.g., a surveillance camera.

ACCESS CONTROLS POLICIES, STANDARDS AND PROCEDURES

Procedures are instructions for users to interface with a system and interpret system information. Procedures are based on policies, which contain mandatory statements about governance, expected behavior and adopted principles. Policies are less fluid than procedures as the latter are used to guide day to day operations. Procedures are written to comply with policies. Because procedures are for people to use, they do not apply to automated functions. How then, do automated functions comply with policies? That compliance is achieved in two ways. First, policy requirements should be included in systems development user requirements and design specifications. The extent of such compliance, however, is often questionable. For example, how long should a password be? To address this, standards can be created. Standards sit between policies and

procedures. They also sit between policies and system specifications. Standards are changed more frequently than policies but less frequently than procedures and system requirements.

Access controls are commonly called information security, especially in the mind of IT people and users. It is often auditors who think of security as access controls because auditors want to tie security to risks and other types of controls.

As stated in Chapter Three, internal controls should start at the policy level. Controls that require manual compliance are in the form of procedures and standards. Controls that require system compliance are in the form of system functions. Controls that are implemented by configuring system software like the operating system and a database management system (DBMS) are set in security standards. Procedures, standards and system functions are based on policies. Some procedures are developed based on policies. Some procedures are developed based on standards which in turn are developed based on policies. The need for a standard depends on the technical nature of policy compliance and the extent of automation. Computer systems logic and configuration are not based on procedures which are manual in nature, instead, they are carried out based on standards.

Information Security Policy

An organization should have an information security policy to define its information security strategy and risk tolerance. This policy will tell employees why information security is important in the organization given the nature of information processed, who is accountable for the information security function, who are responsible for information security and the responsibilities of users. The policy should address infrastructure, software, people and information.
For infrastructure and software, the policy should state the corporate protocol for obtaining approval for security infrastructure and software installation. It should also state the requirements for due diligence security review and testing of infrastructure and software, by referencing to the systems development methodology and software change procedures.

The policy addresses the people component of a system by stating accountabilities and responsibilities. Responsibilities will be codified in standards and procedures. The information component is addressed in the policy by means of providing criteria for defining ownership and assessing risks.

The information security policy as well as supporting standards, guidelines and procedures should be posted on the intranet. New items and significant changes should be communicated to employees by email. There should be training on new policies or procedures to key IT employees and the affected employees in other areas.

The information security policy will need to be supplemented by security standards that address specific risk management and control areas. Examples of standards are password and firewall standards. The following is an example of a corporate information security policy, the Canadian Government's. Only the main body of the policy is shown here.

Treasury Board of Canada Secretariat

www.tbs-sct.gc.ca

Policy on Government Security

1. Effective date

1.1 This policy takes effect on July 1, 2009.

1.2 It replaces the 2002 *Government Security Policy* and the 2004 *Policy for Public Key Infrastructure Management in the Government of Canada*.

2. Application

2.1 This policy applies to:

> All departments within the meaning of Schedules I, I.1, II, IV and V of the *Financial Administration Act* (FAA), unless excluded by specific acts, regulations or Orders in Council.

3. Context

3.1 Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The extent to which government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians.

3.2 Security begins by establishing trust in interactions between government and Canadians and within government. In its interactions with the public when required, the government has a need to determine the identity of the individuals or institutions. Within government, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. Consequently, a broad scope of government activities, ranging from safeguarding information and assets to delivering services, benefits and entitlements to responding to incidents and emergencies, rely upon this trust.

3.3 In a department, the management of security requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response and recovery. The management of security intersects with other management functions including access to information, privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real property, material management, information management, information technology (IT) and

finance. Security is achieved when it is supported by senior management - an integral component of strategic and operational planning - and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours.

3.4 At a government-wide level, security threats, risks and incidents must be proactively managed to help protect the government's critical assets, information and services, as well as national security. Advice, guidance and services provided by lead security agencies support departments and government in maintaining acceptable levels of security while achieving strategic goals and service delivery imperatives.

3.5 The management of security is most effective when it is systematically woven into the business, programs and culture of a department and the public service as a whole.

3.6 Deputy heads are accountable for the effective implementation and governance of security and identity management within their departments and share responsibility for the security of government as a whole. This comprises the security of departmental personnel, including those working in or for offices of Ministers or Ministers of State, and departmental information, facilities and other assets.

3.7 Ministers of the Crown, ministers, and Ministers of State are responsible for the security of their staff and offices as well as the security of sensitive information and assets in their custody, as directed by the prime minister.

3.8 This policy is issued under section 7 of the FAA.

3.9 Treasury Board has delegated to the President of the Treasury Board the authority to amend directives that support the policy in the following subject areas:

- Departmental security management
- Identity management
- Information and identity assurance
- Individual security screening
- Physical security
- IT Security
- Emergency and business continuity management
- Security in contracting

3.10 This policy is to be read in conjunction with the *Foundation Framework for Treasury Board Policies*, the *Directive on Departmental Security Management* and the *Directive on Identity Management*.

4. Definitions

4.1 For definitions of terms used in this policy, refer to Appendix A-Definitions.

5. Policy statement

5.1 The objectives of this policy are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

5.2 The expected results of this policy are:

Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;

Governance structures, mechanisms and resources are in place to ensure effective and efficient management of security at both a departmental and government-wide level;

Management of security incidents is effectively coordinated within departments and government-wide;

Interoperability and information exchange are enabled through effective and consistent security and identity management practices; and

Continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

6. Requirements

6.1 Deputy heads of all departments are responsible for:

6.1.1 Establishing a security program for the coordination and management of departmental security activities that:

a. Has a governance structure with clear accountabilities
b. Has defined objectives that are aligned with departmental and government-wide policies, priorities and plans; and
c. Is monitored, assessed and reported on to measure management efforts, resources and success toward achieving its expected results;

6.1.2 Appointing a departmental security officer (DSO) functionally responsible to the deputy head or to the departmental executive committee to manage the departmental security program, and identifying an executive to participate in setting government-wide security and identity management direction and to represent the deputy head to TBS on all departmental security and identity management activities related to this policy;

6.1.3 Approving the departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation;

6.1.4 Ensuring that managers at all levels integrate security and identity management requirements into plans, programs, activities and services;

6.1.5 Ensuring that all individuals who will have access to government information and assets, including those who work in or for offices of Ministers and Ministers of State, are security screened at the appropriate level before the commencement of their duties and are treated in a fair and unbiased manner;

6.1.6 Ensuring that their authority to deny, revoke or suspend security clearances is not delegated;

6.1.7 Ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence they are investigated, acted on and reported to the appropriate law enforcement authority, national security agency or lead security agency;

6.1.8 Informing TBS of their department's activities related to the development of national or international security and identity management standards, as those activities relate to this policy.

6.2 Deputy heads of lead security agencies are responsible for:

6.2.1 Providing departments with advice, guidance and services related to government security, consistent with their mandated responsibilities;

6.2.2 Appointing an executive or executives to coordinate and oversee the provision of support services to departments and to represent the deputy head to TBS in this regard; and

6.2.3 Ensuring that the security support services provided help government departments achieve and maintain an acceptable state of security and readiness and that those services remain aligned with government-wide policies, priorities and plans related to government security.

> A list of lead security agencies and details on the nature and scope of their responsibilities under this policy are found in Appendix B-Responsibilities of Lead Security Agencies.

6.3 Monitoring and reporting requirements

Within departments

> Deputy heads are responsible for ensuring that periodic reviews are conducted to assess whether the departmental security program is effective, whether the goals, strategic objectives and control objectives detailed in their departmental security plan were achieved and whether their departmental security plan remains appropriate to the needs of the department and the government as a whole.

By departments

> Deputy heads are responsible for reporting periodically to TBS, on the status and progress of implementation of this policy and on the results of ongoing performance measurement.

Lead security agencies

> In additional to monitoring and reporting on their departmental security program Deputy heads of lead security agencies are also responsible for:
>
> Ensuring that periodic reviews are conducted to assess the effectiveness of their security support services to ensure they continue to meet the needs of departments and the government as a whole; and

Reporting on their activities under this policy through current government reporting mechanisms, e.g., Management, Resources and Results Structure (MRRS), departmental performance reports (DPR) and reports on plans and priorities (RPP).

Government-wide

TBS is responsible for:

Monitoring compliance with this policy and the achievement of expected results in a variety of ways, including but not limited to MAF assessments, Treasury Board submissions, DPRs, RPPs, results of audits, evaluations and studies, and ongoing dialogue and committee work; and

Reviewing and reporting to Treasury Board on the effectiveness and implementation of this policy and its directives and standards at the five-year mark from the effective date of the policy. Where substantiated by risk analysis, TBS will also ensure an evaluation is conducted.

7. Consequences

7.1 The deputy head is responsible for ensuring appropriate remedial actions are taken to address issues regarding policy compliance, allegations of misconduct, suspected criminal activity or security incidents, including denying, revoking or suspending security clearances and reliability status, as appropriate.

7.2 If the Secretary of the Treasury Board determines that a department may not have complied with any requirement of this policy or its supporting directives or standards, the secretary of the Treasury Board may request that the deputy head:

7.2.1 Conduct an audit or a review, the cost of which will be paid from the department's reference level, to assess whether requirements of this policy or its supporting directives have been met; and/or

7.2.2 Take corrective actions and report back on the outcome.

7.2.3 Consequences of non-compliance with this policy and its supporting directives and standards or failure to take corrective actions requested by the secretary of the Treasury Board may include recommending to Treasury Board that measures deemed appropriate in the circumstances be imposed.

(End of excerpt from Government of Canada Security Policy)

Information Security Standards and Procedures

An information security policy is at a corporate, high level and generally is not detailed enough for day to day operations and system configuration. Standards and corporate procedures should be developed to take the information security policy to a lower level as a basis for defining system requirements, guiding employee behavior, educating system users, configuring system software and writing operation procedures. Each subsidiary standard or corporate procedure should address a specific subject such as password and firewall. Organizations can refer to professional sources like Control Objectives for Business and Information Technology (COBIT) and International Standards Organization

(ISO) as benchmarks to assess the comprehensiveness of their security standards. ISO 27002 provides guidelines and a framework for organizations to implement information security.

Standards should be supplemented with local procedures that fit each division and computing platform. In addition to standards, there are corporate security procedures for certain areas where there is little fluctuation among operating areas, such as procedures for reporting loss of equipment. The following is a common list of security standards and corporate procedures that large organizations should have.

- Anti-virus.
- Appropriate use of information and information technology.
- Cryptography.
- Data center.
- Disposal of data, media and equipment.
- eBusiness.
- Email.
- Firewall.
- Incident response procedures
- Information classification.
- Intrusion detection and prevention.
- Loss reporting.
- Mobile computing.
- Password.
- Patching.
- Routers.
- Servers.
- Software design.
- Virtual private network.
- Wireless.
- Workstations.

Anti-virus Standard

Anti-virus software is widely deployed in organizations. Tools are controlled by people. Anti-virus software is effective only if IT people properly deploy it and users do not mess around with it. The anti-virus standard should dictate the layers of anti-virus software, the approval for deployment and changes as well as the need to regularly update the virus list (dat file in the anti-virus software tool). Layering means how many levels of anti-virus software protection an email message or a file is subjected to before being opened.

Appropriate Use of I & IT

This security standard should instruct employees as to what kinds of use of I & IT resources are unacceptable in order to support a strong security infrastructure and comply with the overall information security policy. Here is a common list of what is considered unacceptable.

- The use of corporate IT resources for personal purpose to a significant extent.
- Use personal IT resources to conduct corporate business, unless approved by a manager.
- Access, display, download, create, distribute or store any software, graphics, images, text, music, video or other data which are offensive and conducive to a poisoned work environment.
- Use the corporate network for sharing files such as music files, video clips, digital image files or software programs, unless for corporate business.
- Streaming audio or video from the Internet, unless for corporate business purposes.
- Use corporate resources to play games.
- Operate a private business or political activity.
- Misrepresent the organization's views on a matter.
- Discredit others in the organization through electronic communications.
- Send anonymous messages or impersonate others.
- Send chain letters or spams.
- Use offensive, threatening or abusive language in electronic communications.
- Use IT resources to discriminate against or harass, threaten or intimidate other employees or to create a hostile or humiliating work environment.
- Perform unauthorized network scans on, or conduct unauthorized access attempts to corporate systems, applications or services, or spread viruses or malicious code to other systems.

Employees should be educated about this standard upon joining the organization and reminded periodically. For example, a login script can be implemented to pop up a reminder that requires acknowledgement periodically when an employee logs on to the network. This standard should be enforced with system controls such as using a web filtering software system to deny web sites that fall into the above categories and track the types and extent of Internet use. Frequent Internet users should be flagged for reporting to managers who can then assess appropriateness in relation to job requirements.

Cryptography Standard

The Internet has raised security concern in that sensitive information transmitted may be intercepted in the public domain. To mitigate this risk, information can be encrypted. Even information in storage may be viewed by unauthorized individuals when role based access rules are circumvented. Encryption can fill this void. There are many stories about

credit card numbers being disclosed as a result of corporate servers having been hacked. Encryption is based on the mathematical technique of cryptography. It uses a rigorous algorithm and numeric keys. The effectiveness of encryption depends on the robustness of the algorithm and the length of the keys. The cryptography standard should dictate when encryption and encryption related security measures are necessary. It should also define the stakeholders and configuration requirements of the public key infrastructure (PKI). We will describe PKI in more details later. This standard should also specify the strength of algorithms and length of keys.

What is the difference between cryptography and encryption? Cryptography means using mathematics in computer programs to disguise information to achieve security. Encryption means scrambling information with a secret key so that only the authorized people can read the information. Encryption is an application of cryptography. Other common applications include digital signatures, message digest and digital certificates. We will discuss these later.

Data Center Security Standard

A data center carries a high degree of security risk because of the concentration of servers, information transmission and information storage. It attracts a lot of hacker attention. The data center security standard should specify the physical security measures for location of equipment, access levels, locks and surveillance systems etc., commensurate with the significance and mass of servers, data storage and data communication facilities. It should address the location of building site selection and building construction to provide adequate disaster prevention and security breach prevention.

Procedures for Disposal of Data, Media and Equipment

These procedures should instruct management and staff as to the approval levels for disposing of different types of equipment, the disposal log, review of the log, updating inventory records, backing up information and sanitizing the storage media before disposal to prevent the leakage of sensitive information. The organization should adopt a robust disk sanitizing software product that prevents the information from being recovered. Such a product is independent of the operating system in the device being cleansed so that even the operating system logs and configuration parameters are erased.

Where data is stored in an old medium to which the disk wiping software does not apply, the organization should set requirements as to how the medium is disposed of. Examples of such requirements include shredding and sending the medium to a trusted contractor for destruction.

eBusiness Security Standard

We discussed eBusiness infrastructure in Chapter Five and the need to secure the infrastructure. The infrastructure should include security devices. The eBusiness security standard should document the requirements in building the eBusiness infrastructure and provide guidance for mapping the risks of eBusiness to security features.

Email Security Standard

Email is a business critical system because business communication with colleagues, business partners and to a less extent, customers, is done predominantly through email. Just think about what you did last time the email system was down. Being an easy and far reaching tool, email can be abused. Employees may use it to send indecent or illegal material. They may use it for personal purpose to a significant extent, e.g., to such an extent that the majority of email messages are for personal purpose. Organizations should have a standard to tell employees what is not acceptable. The standard should also say when email is not appropriate, e.g., when sending highly sensitive material. Confidential material should be encrypted and the organization should provide the tool and procedures for this.

Firewall Standard

Every organization that hosts a web site should have a firewall to protect its systems against intrusion. Large organizations should have multiple firewalls deployed across business units and in a layered approach to protect the network as the information gets deeper in the organization. A firewall is a security device with rules set by the hosting organization that define what is allowed in and what is allowed out. The firewall standard should provide criteria for locating firewalls, the types of firewall (e.g., rule based vs artificial intelligence), the generic rules, and guidelines for writing specific rules. It should also provide requirements for firewall software update and firewall administration. The logging requirement and associated independent review should also be stated. This standard should define the following:

- Extent of logging
- Log retention
- Change control approval and documentation with respect to rules and configuration
- Firewall administration responsibilities and approval
- Types and location of firewall
- Types of systems supported by firewalls
- Layers of firewall
- Reporting of rule infractions

Incident Response Procedures

Although computers are fast and inherently accurate, its interface with people is not without glitches. Human to human interface is easier to comprehend and problems can be detected more interactively than computer to human interface. In the last chapter, we talked about the risks of computers going down, computer programs being wrong and people misusing information systems etc. These incidents can lead to unreliable information and financial loss. Organizations must have a set of procedures to address incidents.

A large number of incidents are security related. This is why the incident response procedures in many organizations are developed and maintained by the security department. However, the impact on the organization and the urgency for action are often the same between security incidents and non-security incidents. The escalation and remedial action depend on the incident's severity.

Incident response procedures should guide management in determining an incident's severity. For example, it is common in governments to rate an incident as severity level 1, 2, 3 etc. The severity level would call for different amount of resources and different layers of management to be involved in investigation and resolution.
Incident handling usually starts with the IT help desk. In cases where the incident cannot be resolved, procedures should be followed to escalate it to level 2 support. Level 2 support is staffed by subject matter experts. If the incident cannot be resolved there, it should be escalated to level 3 and so on. It is rare for an organization to have more than five levels in terms of technical support because the more levels there are the more bureaucratic the process will become. Meanwhile, the procedures should guide staff to keep management informed on an escalating scale. A sample of these procedures is included in Chapter Three.

Information Classification Standard

Information is the most important component of a system. The extent of infrastructure and software depends on the volume and criticality of information to be processed. Access controls are designed to mitigate the risk related to information availability, integrity and confidentiality. Risk assessment should be consistent throughout the organization. An organization should have a standard that guides managers to classify information based on availability, integrity and confidentiality. Standard labels like levels 1, 2, 3; top secret, secret, confidential; or high, medium, low should be used. Procedures, education, reminders and automated tools should be implemented to support this standard. The standard should prescribe the level of confidentiality, the place of storage and the channel of transmission that require encryption. It should also state when information should not be sent by email. For

example, employee health information should not be sent by Internet email; password reset should be sent in an encrypted email (obviously for passwords used in other than the email system); security diagrams should be encrypted in storage.

Intrusion Detection and Prevention Standard

Firewalls are important preventive controls. Preventive controls are not enough because fool-proof prevention is impractical in order to ensure flexibility and effectiveness of the business environment. Preventive controls should be supplemented with detective controls. The detective complement of a firewall is an intrusion detection system. This device scans allowed traffic and develops a pattern for assessing the likelihood of intrusion. It then either alerts systems administrators to take protective or preemptive actions, or if configured accordingly, the system will take the preemptive actions automatically. When the tool, usually a more advanced tool, is capable of taking preemptive actions automatically, it is called an intrusion prevention system. The intrusion detection and prevention standard contains similar guidance to that in the firewall standard. It states where intrusion detection and prevention systems should be installed, the types of systems (rule based vs artificial intelligence), as well as criteria for rules and device administration.

Procedures for Reporting Loss of Equipment

As equipment and storage media become more portable, they are subject to a higher risk of theft and loss. The loss of hardware results in the cost of replacement, information may be lost if there is no backup. Even with backup, sensitive information may be disclosed. Although it may be too late to prevent such disclosure or information loss, management should be informed immediately to assess the implication and take remedial measures such as informing stakeholders, changing business plans, changing system configuration information so that the leaked intelligence cannot be used against the organization and taking the lesson learned to strengthen procedures. Employees should be instructed on how to report losses and what immediate security measures to take to minimize damage.

Mobile Computing Standard

Employees are increasingly provided with smart phones and laptops. Quite often employees use these devices to send personal email and surf the net for personal purposes. This poses the risks of virus infection, clogging the network with personal messages and exposing the organization to liability if illegal material is sent. To mitigate these risks, an organization should have a standard that defines what types of mobile computing is allowed in the organization and that no personal devices are to be connected to the organization networks unless approved by management. These requirements

should be supported by network configuration and monitoring tools. For example, the standard should say that messages sent over mobile devices for business purpose must be encrypted. The standard should cover inventory tracking of mobile devices. It should also address laptop computer deployment with respect to justification, approval process, physical security, operating system configuration and inventory tracking.

Password Standard

We all have different passwords for different systems. The strength of a password depends on its length, change frequency, complexity and place of storage. The password standard should specify these parameters in relation to the risk of information being protected.

Patching Standard

A worm exploits a computer's software vulnerability, mainly a vulnerability in the operating system. An essential solution to worm infection is to patch the vulnerabilities by installing the fixes released by software vendors. It is important for a large organization to have a standard to specify when patching is to be done, how to prioritize patches when deadlines are tight, how to test the patches etc.

Router Standard

A router is a device that connects two networks or network segments. Many of us have simple routers at home that connect the Internet modem to different devices like computers, printers and voice-over-IP boxes. Routers are necessary for wide area networks and therefore also the Internet. A router has its own operating system which can be configured with different options of parameters. A router also has an address table that governs how data is forwarded, through which circuit and to which IP address. The router standard applies to routers and switches and should indicate the following:

- Authorization framework for parameters and routing table changes.
- Standard configuration parameter values.
- Extent of logging.
- How to locate.
- Periodic review.
- Redundancy, i.e., provision of backup routers.

Server Standard

A server must be physically and logically secured. The standard should specify the physical security necessary depending on the sensitivity of information processed. It should also provide standard configuration parameters for the operating system; which is often called the "standard image". This standard should also provide for inventory tracking.

Software Design Security Standard

Many large organizations have strong infrastructure security but have neglected the need for robust application functions to fend off intruders. This is especially risky against unauthorized access by employees because they don't have to beat firewalls. Application access controls by means of robust design and programming is like homeland security, which is in addition to border control and necessary.

The software design security standard should specify techniques to avoid security holes being programmed that will open back doors to hackers. A back door is a path that leads one to privileged computer resources bypassing the normally required authentication and authorization checks exercised by the relevant applications, operating system and DBMS. Programmers should be required to check the validity and length of values input to prevent buffer overflow (overflowing the real memory in the computer and therefore overwriting program instructions loaded in real memory that could then cause a system to misbehave or shut down). Checking the validity and length of input will also prevent a hacker from injecting System Query Language (SQL) code to query user identity or related information.

Virtual Private Network Standard

Telecommuting is increasingly used to support a mobile work force. Some employees are allowed to work from home. Many organizations give employees remote access to the network to perform system functions that they can perform when they are in the office; one of the reasons for this is to ensure business goes on in the event of a disaster, public transit strike or pandemic. Remote connections increase the risk of unauthorized access because people in the office cannot see who is accessing the network.

Virtual private network (VPN) is a technology that allows people to access an organization's network through the Internet and perform the functions that can be performed as if the person were in the office. That is, the network can be accessed virtually privately using encryption and enhanced authentication. This is not the same as web browsing or eBusiness. In web browsing or eBusiness, the user is restricted to what the web server allows; whereas through a VPN, a user can access everything that s/he can access in the office, e.g., checking pay statements, submitting expense reports and approving journal entries.

The VPN standard should specify the security structure for VPN, the extent of encryption, the depth of authentication, the approval process for users, the applications that are available through a VPN, the logging process, and the monitoring of usage. Some organizations have found that a large number of VPN users have not used the service. Keeping a list of VPN users who don't need the service wastes money and increases security exposure as it unnecessarily increases the number of virtual access points.

Wireless Standard

Organizations increasingly deploy wireless networks to increase flexibility and efficiency. Wireless data transmission is more susceptible to sniffing than wired communication.

The Institute of Electrical and Electronic Engineers (IEEE) has published wireless security standards which have been adopted by network service providers including phone companies and many large organizations. An organization should have a wireless standard to define where wireless can be deployed, the approval process for users to get on the wireless network, applications that are open to the wireless network and which IEEE standard should be followed and when. The latest IEEE wireless security standard is 802.11i, which calls for the Wifi Protected Access (WPA) 2 protocol. WPA2 mainly uses an advanced symmetric encryption algorithm that requires a key length of at least 128 bits for authentication and encryption, called Counter Mode and Cipher Block Code Message Authentication Protocol. The actual key used for message encryption is a derivative of the access point's assigned key, a random number generated by the access point, as well as the MAC addresses of the access point and the remote device.

Workstation Security Standard

A workstation must be physically and logically secured. The standard should specify the physical security necessary depending on the sensitivity of information processed. It should also provide standard configuration parameters for the operating system; which is called the "standard image". The standard should also require inventory tracking.

COMMON ACCESS CONTROLS TECHNIQUES

An information security policy sets the corporate, high level and mandatory requirements for access controls. Compliance with the policy is achieved through infrastructure, software and people. People are guided not only by the policy, but also by standards and procedures. Compliance with the security policy and standards by means of infrastructure and software is achieved by implementing automated security techniques and tools. Here is a list of common access control techniques.

- Access card
- Access control list
- Access log
- Active Directory
- Anti-virus software
- Biometric
- Boundary checking
- Challenged response
- Clean desk practice
- Compliance scanning
- Cryptography
- Disabling unnecessary system software features
- Disk wiping
- File blocking
- File integrity monitoring
- Firewall
- Honeypot
- Intrusion detection system
- Intrusion prevention system
- Locks
- Management or independent review
- Password
- Patching
- Personnel security screening

- Security education
- Security monitoring and reporting
- Single sign on
- Spam filtering
- Staff termination or transfer checklist
- Standard operating system configuration image
- Two factor authentication
- User profile
- Virtual private network
- Vulnerability assessment
- Web filtering
- Web site refresh

We will discuss each of these below.

Access Card

Building and computer room access should be controlled with access cards that contain electronic information to identify the card holder and the facilities that can be accessed. The access control system should be capable of deactivating a card that has been lost or is no longer needed. A change in access privilege such as adding a floor should be done by physically verifying the card and the card holder's identity. Card holders should be required to sign a form upon card issuance committing to inform management when the card is lost and committing not to share the card without management approval. The access control system should track all card usage. Access cards should be coded to indicate the departments where the employees work, the employee classification and the premises where access is to be allowed. Such coding allows the organization to deactivate access privilege with a few clicks for an employee or a group of employees, e.g., locking out unionized employees during a strike. An access card prevents unauthorized access and is a general control as it is applied to physical facilities instead of specific information systems. The security assertions addressed are confidentiality and availability.

Access Control List

Users should be allowed access based on their job requirements. This applies to the breadth and depth of access. Breadth means the extent of information and depth means whether the access is read only, write, delete or all. A system has to be told who to allow access to what and to what depth. This telling is by means of an access control list (ACL). An ACL should first define the system resource, which may be a database table, system function, workstation, router, server or web site. It will then specify who can access the resource and to what depth. "Who" does not have to be a person, it can be a program or system function. For example, the payroll query function cannot update the payroll master file. One can understand ACL better by going to a Windows computer, and finding Windows Explorer, and then right click on a folder and file, going to Security, to see who can access that object (folder or file) and the type (depth) of access. If this is your personal computer, you can define who can access the folder and the type of access, e.g., read, write, delete. The party given access rights can be the administrator, the owner of the file or folder (who created it), any user name (that has a profile in the computer) or a guest (everyone else).

ACL can be applied to any object. Common ACLs are applied in applications, operating systems, firewalls and routers. The subject, i.e., the party with access privilege, may be a user, a computer program, a system function, a job class or a user group. For example, a common ACL is one in a payroll system to restrict the system access to create employee profiles to the payroll administrators. An example of a general control using ACL is to allow only certain computers to go through a router by programming the MAC or IP addresses of the authorized computers on the router.

An ACL is a preventive control as it allows access only based on authorization. It can be applied at a general or application level and satisfies the confidentiality, integrity and availability security assertions.

Access Log

Logging is one of the five security processes. Activity logging allows the events to be reviewed and validated. It also provides a trail for investigation if necessary. Applications, operating systems and other system software products like firewalls should be configured to provide automatic logging. The extent of logging depends on the sensitivity of information. For example, a government system that processes alimony and child support payments should be configured to log all read and write transactions.

The medium used for logging should be reviewed frequently to make sure it is not full. In fact, the system should alert system administrators when the medium is approaching the full mark so that the log can be archived and refreshed. Logs should be reviewed regularly and analyzed to identify exceptions. An example of a log we can all relate to is

the access record of entry to a building. The logging system must enforce review and keep track of the logs that have not been reviewed. Managers should be sent automated reminders to complete the reviews. Organizations should procure reporting software to translate technical logs to user friendly information to facilitate management review and such translation should be validated periodically.

An access log is a detective control and it requires review to detect irregularities. It can be applied at a general or application level and satisfies the security assertion of confidentiality, integrity and availability.

Active Directory

This hierarchical access authentication and authorization structure has replaced the primary domain controllers and backup domain controllers for the Windows operating system. It has the following features:

- Central location for network administration and security
- Information security and single sign-on for user access to networked resources
- The ability to scale up or down easily
- Standardizing access to application data
- Synchronization of directory updates across servers

Active Directory stores all information and settings for a deployment in a central database. It allows administrators to assign system security policies as well as to deploy and update software. Active Directory networks can vary from a small installation with a few computers, users and printers to tens of thousands of users, many different network domains and large server farms spanning many locations. Active Directory contains information about users, user groups, roles and access privileges etc. It is a formal structure of ACLs along with user authentication credentials. Active Directory is a preventive control and it supports all security criteria.

Anti-virus Software

This is a "must have" internal control in every organization. The main reason viruses cause less headache for management today than say, a decade ago, is that anti-virus software is more rigorous. The software includes the virus detection and cleansing software engine and a user interface. Virus detection is performed mainly by comparing the suspected virus to a virus signature file in the software. The virus signature file, called a dat file, contains the signature of each active virus, i.e., a virus that is known to have propagated and still has a significant potential to travel in the Internet community. So what is a signature? Anti-virus software should be capable of detecting viruses and worms.

A virus signature is in some ways similar to a human signature. To be more precise, it consists of a unique identification of the virus. However, unlike human signatures, a virus signature is not created by the virus writer. It is not an agent that allows the virus to multiply. A virus multiplies by way of sending itself to different computers either by email or another widespread Internet channel.

When a virus propagates, anti-virus software vendors study the virus as to what damage it can do and how the damage is done. It looks for a sequence of bits in the virus that can uniquely identify it. The length of this sequence should be long enough to prevent false positive but also not too long so as to quickly trap a virus. This sequence is called the signature. The vendor then adds this signature to the signature file that contains thousands of virus signatures, i.e., for the viruses that are still active. The anti-virus software vendor also updates the repository of virus description available on its web site that talks about the extent of propagation and pay load (damage) of each active virus.

Anti-virus software vendors make the signature file available for download by its customers. In fact, most organizations have configured the anti-virus software to check the vendor's site to download the latest file. The customary practice is daily checking.

When a virus is found, the software will remove the virus from the infected file. The anti-virus software tool can also be configured to quarantine the infected file instead of removing the virus to allow the user organization to study the infected file for, e.g., forensic purpose. How does the anti-virus software know there is a virus? Well, every program file, including a Word or Excel macro, will be scanned for comparison with the signatures. If there is a match, that program file or macro is deemed to be infected and the virus removal or file quarantine action will be engaged.

Organizations should have a standard configuration for anti-virus software and instruct users not to change the settings. Anti-virus software should be installed at multiple layers for redundancy to achieve defense in depth. In a large organization, there should be three layers, which have to do with the fact that viruses mainly infect by email.

Anti-virus should be installed on the Internet email server to scan all incoming Internet mail. It should also be installed on the local email servers to scan internal email and Internet email that has passed the Internet email server. The latter will provide redundancy, i.e., an extra level of protection in case the Internet email server anti-virus software is not up to date. Finally, anti-virus software should be installed on every server and every workstation. This is to detect any virus that does not come through by email or that comes in by email and has somehow bypassed the Internet email server and the local email servers virus scanning.

When a virus or worm is detected, the organization should disconnect the computer from the network to prevent further infection. It should then remove the malicious software and patch the computer to close the vulnerability. After that, it should scan the computer again for viruses or worms. Then, if the scan does not reveal any infection, the computer can be re-activated and reconnected.

Although anti-virus software detects viruses, it is a preventive control as it stops a virus from infecting a computer. Because the email system is common to all employees, anti-virus software protects the infrastructure and is a general control. Anti-virus software addresses the authorization stage of the access control cycle and supports the confidentiality, integrity and availability attributes of security.

Biometric

This authentication method is increasingly used despite privacy concerns. For example, in Japan, a large number of ATMs use biometric. Many PCs and laptops are equipped with fingerprint authentication for login.

Organizations should assure users such as customers and employees that the biometric will be secured and used only for the purpose of authenticating the user in the specific system disclosed when the biometric was captured. To apply this method, the organization first has to capture the biometric. The biometric will then in recorded in a user profile and stored in a secure authentication server. When the user shows his or her biometric, e.g., palm print, the capturing device will digitize the image and send it to the server for comparison. If there is a match, the user is allowed access. Biometric should be encrypted when not in use. When a device needs to access a biometric, it sends an encryption key to decrypt the information. The server must be hardened to prevent hackers from swapping credentials.

Advancing technology is reducing the chance of false positives or false negatives to a negligible degree. Capturing devices must be capable of detecting artificial images of biometrics, e.g., a plastic finger. For example, in addition to reading the finger print pattern, the device can check the temperature, humidity and pulse of the finger.

Biometric is a preventive control as it serves the authentication function. It can be applied at a general or application level. The security attributes being supported are confidentiality, integrity and availability, depending on the system capability of the resource being protected with biometric authentication. The relevant security process is authentication.

Boundary Checking

This web based control is used to prevent SQL injection and buffer overflow. It restricts the length of data input to prevent insertion of commands that will cause system misbehavior.

Boundary checking is a preventive control as it prevents invalid data input. It is usually applied at an application level because such checking has to be part of the application's web interface. It covers the authorization stage of the access control cycle and addresses mainly the integrity security attribute.

Challenge Response

Sometimes when we register as a user on a web site, we are asked to choose or compose a security question and provide the answer. Later on if we have to access the web site to obtain sensitive information, we might be asked to provide the same answer. Answers are case sensitive. If our answer differs, our request is denied. This method of authentication is called challenge response. Another application of challenge response is to ensure that the access is being attempted by a human being as opposed to an automated agent like a robotic tool. In this application, the user is asked to read some letters in skewed, disproportional or italicized fonts and type it in a box. The challenge response method can be applied at the application or general level. It is a preventive control and supports all three security attributes of confidentiality, integrity and availability because the system being protected may contain confidential information, information that must not be compromised and be a critical system that must be available all the time. The relevant security process is authentication.

Clean Desk Practice (Policy)

Sensitive information in memory disks and on paper are often compromised because people leave them unattended in their office for an extended period. They would not leave money or their wallets on their desks like that. Organizations should tell employees that they must maintain "clean desks" and regularly remind people of this. Security staff members should conduct periodic observation and then focus their security education based on results of observation. If it is found that highly sensitive documents are left in the open, the employee's supervisor should be informed.

Compliance Scanning

An organization's security policies and standards should be implemented in hardware and system software consistently using standard images across the enterprise. Every computer should be configured using a baseline of minimum security parameters. Certain sensitive servers can surpass the minimum configuration. System configuration should be scanned periodically using software tools for compliance with policies and standards. The scanning should be performed by people who have no system administration responsibility in order to be objective. Compliance deviations should be reported to management and followed up for correction.

Compliance scanning is a detective control and it can be applied at an application or general level depending on the scope of the system software being scanned. It covers the authorization stage of the access control cycle and addresses all three security attributes of confidentiality, integrity and availability. The relevant security process is monitoring.

Cryptography

Cryptography is a technique to code and scramble data to prevent it from being read or changed without authorization. It enables information to be stored or sent across communication networks without losing confidentiality or integrity. Cryptography uses complicated algorithms and numeric keys. Its effectiveness depends on the rigor of an algorithm, the length of the keys and the security over the keys against unauthorized use. The common applications of cryptography are message digest, data encryption, digital signature and digital certificate. Each of these mathematical applications can be used in a variety of business scenarios.

Message Digest

Usually, cryptography is used to protect confidentiality so that only the intended recipients can read the data and that is achieved with data encryption. Where confidentiality is not the only concern and integrity must be preserved, a form of cryptographic function called message digest can be used. A message digest is a hashed version of a document or a message, determined using a hashing algorithm. Hashing algorithms are complicated. To help understand its nature, one can relate it, in a simple way, to dividing the raw data (binary representation of numbers, text or pictures) into a long prime number. A prime number, especially a very long one helps to ensure uniqueness.

When the recipient wants assurance that a long document or message has not been changed along the way, a message digest can fulfill this need. The sender's computer uses a hashing algorithm to compute a message digest and sends it along with the document or message. The recipient's computer uses the same hashing algorithm to compute the message digest and compares it to the message digest received. If there is no difference, the recipient has assurance that the document or message has not been changed along the way, say, by a hacker.

The hashing algorithm computes a fixed length message digest from an original data string. The length of the digest depends on the algorithm and ranges from 128 bits to 512 bits, regardless of the length of the original data string. Because most documents or messages are longer than 512 bits, in theory, some different documents or messages will be hashed to the same message digest; i.e., the relationship is many to one. This lack of uniqueness casts some concern with respect to the reliability of a message digest, i.e., how does one know that a message digest for a document is actually the true message digest or is it really the message digest of another document? The proximity to uniqueness, or the reliability, of a message digest depends on its length. A 512 bit digest is more reliable than a 128 bit digest. However, the longer the digest, the slower the process is in hashing. Another factor in reliability is the sophistication of the algorithm. Current hashing algorithms use hash lengths of up to 512 bits. Common hashing

algorithms are Secure Hash Algorithm and Message Digest. To prevent a hacker from changing the document in transit and substituting the hash, both must be sent using different channels that are highly difficult for a hacker to link the two objects.

Even with a 128 bit hash, the number of different hash values is 2^128, or 340,282,366,920,938,463,463,374,607,431,768,211,456. Although there is no theoretic uniqueness in a message digest, with such a large number of hashes, it is extremely unlikely that two documents prepared at random will be hashed to the same value. This cryptographic process is irreversible, i.e., a message digest cannot be used to recreate the original document or message, so as to prevent hackers from doing reverse engineering to determine the actual document or message from the message digest.

A key property of a hashing algorithm is that it must be structured such that a minor difference between two plain text data strings, when hashed, will produce two hashed strings that are different, but not necessarily just different in a minor way like the original data strings. This property makes it difficult for a hacker to reverse engineer.

A message digest algorithm should have the following properties:
1. Every bit of the hashed value is influenced by every bit of the plain text value.
2. If any bit of the plain text changes, every output bit has a 50% chance of changing.
3. Given a hashed value and its corresponding original plain text, it should be computationally infeasible to find another plain text string with the same hashed value.

Message digest is a preventive control. It prevents spoofing and covers the authentication stage of the security cycle. The security attribute addressed is integrity.

COMMON BUSINESS APPLICATIONS OF MESSAGE DIGEST

Now, you understand the mechanics of a message digest. What are the business applications? There are two common applications.

An organization that wants to post a critical document on the Internet or deliver it to another party may be concerned that the document might be changed by a third party or altered because of network noise or errors. A message digest can be used to confirm that the document has not been changed. The posting or sending organization will compose a message digest of the document before delivering it. It can then deliver the document and the message digest separately. The recipient can then recompute the message digest using the same algorithm and verify with the message digest received. If the two message digests match, there is assurance of the integrity of the document. If the document is posted on a web site, the posting organization can download it and recompute the message digest, and then compare it with the message digest computed before posting. The two message digests should match. This is a good technique to periodically check the

integrity of web site content to detect even a minor but critical change by a hacker, e.g., a key word in a contract or system description. Comparing two message digests is faster than comparing the content of the two web sites

The second application of a message digest is actually related to the first one. Instead of or in addition to ensuring integrity, the sender of a message may want to assure the recipient that the message is actually sent by him or her, not by someone who pretends to be the legitimate sender. As we discussed earlier, it is not difficult for a technical person to send out email as someone else. This is called email spoofing. To mitigate this risk, a message digest can be composed and then encrypted to form a digital signature. The digital signature will be sent along with the message. The recipient can then verify the digital signature to confirm that the message actually came from the purported sender. We will discuss digital signatures in more details later in this chapter. Confirming that a message was actually sent by the purported sender makes the message unrepudiatable, i.e., the sender now cannot deny having sent the message because the digital signature has been verified by the recipient.

There are other applications of message digest. An interesting one is to use it to competitive bidding. Bidders are often concerned about the security over their bids after submission, i.e., submitted bids are leaked to competing bidders who will then tailor their bids to win. One way to alleviate this worry and enhance transparency is to require the bids to be submitted in a hash form. After the deadline for the hash submission, the hosting company will ask for the same bids in encrypted form. The company hosting the bidding process will decrypt the bids for evaluation. Once a winning bid is determined, the hosting company will hash the winning bid and compare to the submitted hash. If there is no match, the winning bid is disqualified and the next highest scored bid will be hashed and compared to the submitted hash, it there is no match, the next bid will be considered etc.

Data Encryption

When sensitive information is transmitted in an inadequately secured channel or stored in a less than secure place, the information sender, owner or custodian may wish to encrypt it to prevent unauthorized viewing. When encryption is used, an algorithm transforms plain text into a coded equivalent, known as cipher text, for transmission or storage. The coded text is subsequently decoded (decrypted) at the receiving or retrieval end and restored to plain text.

Encryption uses an algorithm and a key to turn plain text into coded information which cannot be decoded without the same algorithm and the appropriate key. A key is used to make encryption unique to the same user or a small group of users. The purpose of encryption is to enable only the authorized users to read the data, so the encryption algorithm must be reversible, i.e., what is encrypted must be decryptable to the

authorized parties. Because of decryptability and most encryption algorithms are commonly accessible, a key is necessary, in addition to the algorithm, to prevent encrypted data from being decrypted by just anyone.

The key is randomly generated by encryption software and it consists of a bit string that generally ranges from 56 bits to 2,048 bits. Like a password, the longer the key and the more frequently it is changed, the more difficult it is for an intruder to break the encryption. Safeguarding the key is also critical; for example, a key recorded in a computer without strong password protection serves little value in protecting the stored data; a similar weakness is to store a smart card holding the key in the same bag with the computer.

There are two types of encryption algorithm: symmetric and asymmetric. A symmetric algorithm uses the same key to encrypt and decrypt. An asymmetric algorithm uses a pair of keys, one key to encrypt and the other key to decrypt.

Encryption would be invaluable when a computer or a disk falls into the wrong hands, to keep the data protected. News about credit card numbers being exposed to hackers by merchants points to the importance of stored data encryption. Some companies store credit card numbers in plain text.

Individual files or folders can be encrypted. Organizations are increasingly deploying hard drive encryption software that encrypts the entire hard disk instead of leaving it to the user to decide what files to encrypt. A pass phrase should be configured to invoke decryption. Portable devices like removable disks and USB keys can be purchased with encryption software resident in the devices.

Encryption software should be configured to allow a limited number of pass phrase attempts before the pass phrase is invalidated and hence the data cannot be decrypted. There should be a key recovery process to guard against legitimate failure to enter the correct pass phrase, administered within the organization. If a thief steals a laptop and fails to enter the right pass phrase, say, after five trials, the disk becomes useless.
A common key recovery process involves a key escrow within the organization. Access to the backup key (a copy of the actual key) should require strong authentication with the password immediately changed and the number of people having access should be highly restricted. A reliable method is to encrypt the backup key or to break the backup key into pieces in different encrypted escrows.

Encryption prevents unauthorized viewing and can be applied at a general or application level depending on what is encrypted. It addresses the confidentiality security attribute. The relevant security process is authentication.

Symmetric (Private) Key Encryption

In symmetric key algorithms, the same key is used to encrypt and decrypt the data. This private key must be kept secret for the information to remain secure; thus, a different shared key is required for each pair of users. Using the same key at both ends simplifies the process, however, that makes it very important to safeguard the key. A symmetric key typically ranges from 56 to 256 bits long. A major drawback of using symmetric keys is that the number of keys to maintain can be unwieldy. Here is an example.

Two people who communicate with each other using encryption can use the same key. Three people who communicate secretly with each other should not use the same key, otherwise, the value of encryption starts to erode. For three people, Al, Bill and Cherry to use unique symmetric keys, Al will need 2 keys, one for communicating with Bill and another for communicating with Cherry, Bill and Cherry will also need 2 unique keys each; however, there is some overlap, because the 2 keys used by Al can also be used by Bill and Cherry, i.e., the key between Al and Bill is the same as the key between Bill and Al. So for a group of 3 people, we need 3 keys. For a group of 4 people, we need 6 keys, so far the number is quite manageable. The formula for calculating the number of keys needed is (n x n - n) / 2, with n being the number of parties in the group. For an organization with 60,000 employees who communicate with each other using encrypted email, the number of keys is 1,799,970,000; it can be difficult to manage. This formula is based on combinatorial mathematics because a symmetric key is used by two parties and since both parties have to know the same key, order does not matter, so it is the number of combinations of 2 in a group of n users that determines the number of keys needed, not the number of permutations.

The above analysis seems to suggest that symmetric key encryption is impractical. That is not true. Temporary keys are often used to encrypt data that travels on the Internet, for example, for eBusiness. Because such a key expires as soon as the user logs off or exits the web site, there is no need to maintain a large file of keys and the key management overhead described above does not apply. Common symmetric key encryption protocols include Data Encryption Standard (DES, 56 bit key), Triple DES (56 bit key applied three times), Wifi Protected Access (128 bit or 256 bit key) and Secure Socket Layer (128 bit dynamic key). Secure Socket Layer is used in eBusiness.

Asymmetric (Public) Key Encryption

The other major type of algorithm in popular use is public key encryption, which is based on a pair of keys: a private key and a public key. Something encrypted with one of the keys can be decrypted only with the other key. Generally, the public key is used to encrypt data and the private key to decrypt. The two keys with equal length but different values are generated by the same algorithm simultaneously and therefore mathematically related. However, the algorithm is asymmetric, so knowing one key is no help in being able to derive the other. A user wanting to receive confidential information can therefore freely announce his or her public key, which then is used by the senders to encrypt data.

The data can be decrypted only by the holder of the corresponding private key. The private key is usually stored on the hard disk. It can be stored in a memory disk or a smart card. It is not memorized because the user is not asked to key it in.

The public key system reduces the number of keys to be managed because each user needs only two keys regardless of the number of parties involved in communication. Compare this with the symmetric key system, where a unique key has to be used to communicate with each person. The number of keys needed for a group of n parties to communicate with each other using the public key system can be calculated as 2n. So for an organization with 60,000 employees, only 120,000 keys have to be managed, as opposed to 1,799,970,000 under the symmetric key system.

In a public key system, it is critical to ensure that the public key is authentic and really belongs to its announced owner. A public key can be attached to a digital certificate, which serves to authenticate the public key. We will discuss digital certificate in more detail later in this chapter.

Asymmetric keys are typically 2,048 bits long. They are longer than symmetric keys because to prevent a hacker from deriving the private key from the pubic key, more rigorous mathematics is used. Public key (asymmetric) algorithms are therefore slower to execute than symmetric-key algorithms. Common asymmetric algorithms are RSA (Rivest, Shamir and Adleman) and Diffe Hellman. Canadian and United States governments require that asymmetric keys be at least 2,048 bits long each to be acceptable for government applications. Another reason for asymmetric keys to be longer than symmetric keys is that a hacker can use a public key to launch a plain text attack as follows.

Using the algorithm and a public key, a hacker can encrypt different plain texts that are similar to the actual encrypted texts being transmitted by genuine users. The hacker can then compare the self generated encrypted texts to the intercepted encrypted texts. Once there is a match, the hacker knows the plain text equivalent of the intercepted encrypted text. In a symmetric algorithm, plain text attack is much more difficult if not impossible, because the hacker has to try different keys to encrypt the text and as we said earlier, a 128-bit key will take a long, long time for a hacker to guess with computers.

Public-Key Infrastructure

A public-key infrastructure (PKI) is the underlying technical and institutional framework that allows public key encryption technology to be deployed widely within an organization and between organizations. It includes policies and procedures, the infrastructure to manage keys, key owners and the key recovery process in case of loss of a key. A common tool to manage keys and key owners is a key directory. There are commercial software packages for such a tool. Often keys are shared between

organizations, so it would help to have a standard protocol for key management and searching. One such protocol is Lightweight Directory Access Protocol (LDAP). It is called "lightweight" because it is easier to implement.

PKI is a general control as it applies to multiple applications. It is also a preventive control as it helps preserve confidentiality and integrity. The security process of authentication is covered.

Digital signature

The public key system also allows the sender of a message to digitally sign the message by using his or her private key. The recipient can authenticate this signature by using the sender's public key. Digital signatures are difficult to counterfeit and easy to verify, making them superior to handwritten signatures. A digital signature is established by creating a message digest of an electronic communication, which is then encrypted with the sender's private key. A recipient who has the sender's public key can verify that the digest was encrypted by the sender and therefore also find out whether the message has been altered by a third party. Here's how it works.

1. David wants to send a message to Elaine, "Will you marry me?"

2. Elaine has told David to digitally sign messages about their relationship so she knows they are really from him.

3. David's computer will first create a message digest of the actual message.

4. The message digest is then encrypted using the David's private key to form the digital signature.

5. The digital signature is now sent along with the message.

6. When Elaine receives the message and the digital signature, her computer also creates a message digest by hashing the actual message using the same algorithm.

7. Elaine's computer uses David's public key to decrypt the digital signature. Because the digital signature was created by encrypting the message digest using David's private key, by decrypting the signature, Elaine should arrive at the message digest created by David's computer. Now Elaine has the message digest David composed.

8. In step 6, Elaine has also independently composed a digest of the received message.

9. Elaine's computer then compares the independently computed message digest with the decrypted digital signature. The two should match. It they do, Elaine's computer has confirmed that the digital signature is genuine, or that the message was actually sent by David.

10. If there is no match, Elaine's computer will alert that the digital signature cannot be verified and the inference then, is that the message was not sent by David.

Digital signatures can be applied to email messages, electronic documents transmitted, software downloading and software distribution. The purpose is to provide assurance that the source is authentic and the content has not been changed during transmission. Programs and data files can be digitally signed to enable the users to authenticate the files for origins and authors. Digital signatures have legal recognition.

A digital signature addresses the security criterion of integrity. The relevant security process is authentication. Some organizations use digital signature and encryption to authenticate and protect DNS lookup requests and IP addresses, for internal IP addresses tied to highly sensitive servers.

Digital Certificate

A digital certificate is an electronic business card used on the Internet to certify that a web site being visited or the party conducting eBusiness is who s/he or it claims to be. It is generally used in secure Internet connection. When a user accesses a web site that requires encryption, a digital certificate is transmitted by the web site to the user. The user's browser can then confirm the authenticity of the digital certificate and stores the certificate on its hard disk for future reference. The digital certificate includes, among other information, the certificate owner's public key and the digital signature of the organization that issued the digital certificate.

Most digital certificates of large organizations are issued by independent organizations. This is analogous to an education certificate issued by a university to a graduate. A certificate issuer is called a certificate authority (CA). To assure the certificate holder and other users that the certificate was actually issued by the CA, the CA digitally signs the certificate. Two major CAs in North America are Verisign and Entrust.

A CA charges a fee for the certificate and exercises due diligence to assess the authenticity of the web site including a limited security review, interviews with management, financial review as well as confirmation and collaboration with third party information like industry regulators, to ascertain that the organization requesting a certificate is who it claims to be and that the server where the certificate will be placed is owned by the web hosting organization and secured. The CA also provides the software

for key generation and processing. A CA may be internal. For example, a government may issue certificates to servers for secure intranet, or to users for authenticating the users. Most organizations that conduct eBusiness with customers engage commercial CAs.

Where the data being transmitted between the web site and users are less sensitive but still encrypted, the web site may use a self issued certificate. For example, many universities use self issued digital certificates and simply use the web hosting software tool like Apache or Microsoft's Internet Information Server to generate the certificate and the asymmetric keys. Sometimes when you access a university web site for its hosted web based email system, you might get a warning from your browser that the digital certificate cannot be authenticated. People who access such an organization frequently usually ignore such warning, and that may be OK when you are not providing credit card, financial or other sensitive information. Such a self-issued certificate cannot be authenticated because the user's browser does not have the web site's public key to verify the signature or because the certificate has not been digitally signed.

A digital certificate typically contains the following information:

1. Serial Number: Used to uniquely identify the certificate.
2. Subject: The person, or entity identified.
3. Signature Algorithm: The algorithm used to create the CA's digital signature.
4. Issuer: The entity that verified the information and issued the certificate.
5. Valid-From: Valid-To: The expiration date. The date the certificate is first valid from. A certificate is seldom longer than two years. The longer a certificate is for, the higher the risk that the certificate owner's authenticity has deteriorated without the knowledge of the CA, in which case, the certificate is misleading.
6. The web site's public key.
7. The CA's web site.
8. Issuer's (CA's) digital signature.
9. The algorithm used to hash the digital certificate to produce the digital signature.
10. It may also contain the CA's public key.

How does a browser use a web site's digital certificate? Upon downloading the digital certificate, the browser will check whether the certificate is the same as that stored on the hard disk. If so, it has authenticated the certificate before and the certificate has not changed. If not, it will verify the CA's digital signature. Most browsers have the public keys of major CAs like Verisign and Entrust. As stated above, a public key is used to verify a digital signature.

How is the digital signature verified? The user's browser uses the CA's public key to decrypt the signature to arrive at the message digest of the digital certificate. It then uses the hashing algorithm stated in the certificate to hash the certificate to form a message digest. The two message digests are then compared. If they agree, the CA's digital signature has been verified and the digital certificate is deemed to be authentic. The browser then stored the certificate on the hard disk.

Once the web site's digital certificate has been verified, the browser uses the web site's public key for secure eBusiness. Some web sites require users to have digital certificates. Organizations that give their employees remote access to corporate systems through a virtual private network (VPN) may require employees to use personal digital certificates issued by the organization. Another example where user digital certificates are required is secure electronic transactions (SET). Under SET, a bank issues digital certificates to customers and merchants for the purpose of authenticating the merchants in credit card transactions. We will discuss VPN and SET in more detail later in this chapter.

A digital certificate prevents malicious web site spoofing or redirecting as it assures the user that the user is accessing the web site s/he intends to access. It can be applied at a general or application level depending on the business scope of device that is being certified. It covers the authentication stage of the security cycle and addresses the confidentiality and integrity security attributes depending on the access capability of the device being certified.

E-business Encryption

Secure Socket Layer (SSL) is the de facto encryption standard for eBusiness encryption. Here's how it works.

1. A user accesses a web site that requires encryption. Encryption is enforced by the web site, not a user.
2. The browser downloads the digital certificate from the web site.
3. The browser checks the hard disk to look for an identical digital certificate.
4. If there is a match to a stored digital certificate, the browser trusts the web site and goes to step 13.
5. If there is no match, e.g., this is the first time the web site is visited from the computer being used, the browser checks the downloaded digital certificate to determine the identity of the CA and reads the certificate's digital signature and the CA's public key.
6. The browser retrieves the CA's public key from a file in the browser. If the browser does not have the CA's public key, the browser goes to the CA's web site to download it. The browser compares the independently obtained CA public key to the one stated on the digital certificate (if it is stated). If there is a difference, it does not continue to authenticate the certificate and it alerts the user that the certificate cannot be authenticated; the browser does not continue with the transaction. If the browser has the CA's public key or if the downloaded CA's public key does not conflict with the CA's public key on the digital certificate, the browser proceeds to step 8.
7. If there is no matching certificate in the hard disk and the downloaded certificate is not signed, the browser gives the same warning to the user as in the last step. If the user decides to ignore the warning, the unsigned certificate is stored in the hard disk, and the browser continues with the transaction.
8. The browser uses the CA's public key to decrypt the digital signature.
9. The browser uses the hashing algorithm stated in the digital certificate to hash the digital certificate.

10. The browser compares the decrypted digital signature with the hash.
11. If the two match, the browser has authenticated the digital certificate and trusts the web site. The certificate is stored on the hard disk.
12. If the hash computed by the browser does not match the decrypted digital signature, the browser warns the user that the site is not trustworthy and does not continue with the transaction.
13. The browser generates a 128 bit symmetric key.
14. The browser uses the web site's public key to encrypt the 128 bit symmetric key.
15. The browser sends the encrypted symmetric key to the web site.
16. The web site uses its private key to decrypt the 128 bit symmetric key.
17. All data transfers between the browser and the web site are encrypted and decrypted using the 128 bit symmetric key.
18. If the web site asks the browser whether it has a digital certificate issued by the web site for the user, i.e., a customer (consumer's digital certificate), the browser looks up the user's digital certificate and provides it to the web site. This certificate is seldom used and its main purpose is to authenticate the user. It is impractical as it creates overhead for the merchant and makes eBusiness less portable for customers.
19. If the user has a customer digital certificate issued by the merchant's web site, it sends the certificate to the merchant. The merchant which issued the customer digital certificates should require the customers to use pass phrases to activate the digital certificates every time they are used.
20. The merchant's web site then authenticates the customer's digital certificate with the customer's public key which was generated by the merchant's web site and kept there.
21. When the web site is closed by the user or when the user logs off from the web site, the 128 bit symmetric key is discarded by the browser and the web site.

Because of the short life and the length of a 128 bit symmetric key used in eBusiness, it is believed that such a key has not been broken by hackers. There are 2^128 different values of a 128 bit key, or 340,282,366,920,938,463,463,374,607,431,768,211,456 different keys. It is estimated that it would take a powerful computer 10 years to break a 128 bit key. Why don't the web site and the browser just use the web site's public key for data encryption? There are two reasons.

First, an asymmetric algorithm is much slower than a symmetric algorithm and the system performance impact is significant considering the large amount of data being transmitted; e.g., someone can stay on a web site to do account enquiry, make purchases or trade stocks for hours.

Secondly, even if the browser can encrypt data using the web site's public key and the web site can decrypt it using its private key, what key will the web site use to encrypt data to be sent to the browser? A typical browser is not capable of generating a key pair. Even if it can, a web site will have to keep track of the public keys of numerous and an uncontrollable number of users because anyone can access a web site to make purchases.

How do you know a web site has enabled encryption? There are two ways. First check the URL at the top to see if it starts with https, if so, there is encryption. The letter "s" stands for secure. Secondly, look for a lock at the top of the screen.

Ebusiness encryption is a preventive control. It is an application control because encryption is enabled by the merchant on an application by application basis. The security assertion of confidentiality is addressed and the relevant security processes are authentication and authorization.

Email Encryption

In most large organizations, the email security policy or standard provides criteria for securing email by means of encryption and digital signature. The corporate email system should support it. For example, the security policy may say that information rated as "medium" sensitive must be encrypted when sent outside the organization by email. Email messages generated by a corporate email system like Microsoft Outlook and destined for a similar email system, i.e., email applications using the Simple Mail Transfer Protocol (SMTP) like Outlook, can be encrypted using public keys. They can also be digitally signed using private keys. There are four degrees of security when sending email.

An email message can be sent:
in plain text,
encrypted,
digitally signed or
encrypted and digitally signed.

Let's explain the process for email encryption and signature.

1. Frank wants to send an encrypted and signed message to Gail.
2. Frank's computer is equipped with software to generate an asymmetric pair of keys.
3. Gail's computer is equipped with software to generate an asymmetric pair of keys.
4. Frank's computer generates the key pair and stores both keys on the hard disk.
5. Frank's computer sends the public key to the organization's PKI directory for sharing with other users.
6. Frank can also send the public key by email to friends or post it on a web site.
7. Gail will also perform the last three steps.
8. If Frank wants to encrypt an email message to Gail, Frank's computer encrypts the email with Gail's public key. The email program fetches Gail's public key from the PKI directory.
9. If Frank wants to digitally sign an email message to Gail, Frank's computer prompts Frank for a pass phrase.
10. If the pass phrase is accepted, Frank's computer creates a message digest of the email message and encrypts it using Frank's private key to form a digital signature.
11. Frank's computer then sends the encrypted and signed email message to Gail.

12. When Gail opens the message, the computer realizes it is encrypted. It prompts Gail for a pass phrase.
13. If the pass phrase is accepted, Gail's computer decrypts the message with Gail's private key.
14. Gail's computer also recognizes that the email message is digitally signed.
15. Gail's computer creates a message digest from the email message.
16. Gail's computer fetches Frank's public key from the PKI directory and uses that key to decrypt the digital signature.
17. The decrypted digital signature now becomes the message digest that Frank's computer composed before sending the message.
18. Gail's computer compares the message digest it has computed with the decrypted digital signature.
19. If the two values match, Gail's computer is assured that the email was actually sent by Frank and it has not been altered along the way.
20. If there is no match, Gail's computer alerts Gail that the digital signature cannot be verified. There should be a link for Gail to click on to find out what the alert means.

How does an email program like Outlook generate encryption keys? The answer is it doesn't. It can only apply the keys in encryption and digital signatures. The keys are generated by encryption software which can be ported to Outlook. Large organizations will buy and implement the software as part of their public key infrastructure (PKI). A small organization may buy encryption software that does not require a PKI, e.g., Pretty Good Privacy, which allows two users or organizations to exchange and authenticate their public keys respectively. Public keys should not be exchanged in plain text Internet email otherwise they are subject to person-in-the-middle attack, as explained below. PGP uses an even more rigorous process of encryption than what is described above. It generates a session key like an eBusiness SSL session key for encrypting and decrypting email. It lets the sender encrypt the session key with the recipient's public key and sends the encrypted session key along with the encrypted email.

The above process does not apply to Web mail like Yahoo, Hotmail or university provided email accounts over the Internet. The encryption used for web mail is based on the SSL protocol, like that used in eBusiness. A web mail operator may enforce encryption for the entire session or only for the password. Digital signatures are generally not available in Web mail. This is because to enforce digital signatures, the sender and the recipient have to each possess a key pair, private key and public key. As we discussed under eBusiness encryption, it is impractical for a web site to require customers to have a key pair.

Not only does SMTP encryption prevent unauthorized viewing, it mitigates the risk of accidentally sending sensitive email to the wrong person. For example, if one wants to send an encrypted email message to david.c.chan@ontario.ca, but inadvertently types david.chan@ontario.ca, and the sender does not have David Chan's public key, the email program will notify the sender that the public key cannot be found; this should alert the sender to correct the address. On the other hand, if the sender does not encrypt the email message, it will go to David Chan by mistake, instead of being sent to David C Chan.

The importance of email in terms of confidentiality is sometimes underestimated. It is no longer used just for message transmission. Instead, it is increasingly used to transmit business transaction data like insurance policy applications. Email is a business critical system.

Email encryption is much less frequently used than eBusiness encryption for two reasons. First, unlike eBusiness encryption which is invoked by the merchant and requires no action by the customer, email encryption other than web mail requires the sender to invoke encryption or digital signature and that usually involves a couple of extra clicks and a pass phrase. Secondly, the recipient may not have encryption software installed or a key pair. Because most recipients do not have email encryption software installed, the default practice of senders is to send plain text email even if the sender has encryption capability. It is important for organizations to remind users to encrypt and digitally sign highly sensitive email and to refrain from sending such information by email if encryption is impractical. There should be criteria to define sensitivity. Sensitivity, for the purpose of deciding whether to use encryption, mainly has to do with confidentiality. Examples of highly confidential information are health information, business plans, contracts and documents related to litigations.

For SMTP mail, a digital signature is more frequently used than encryption between two organizations. This is because the sender does not need the recipient's key to sign email. There are some small certificate authorities (CA) that provide certificates to email users to enable them to digitally sign emails; the certificate is sent along with the email so the recipient can authenticate the digital signature. If the certificate does not have the CA's

URL, the recipient's email program cannot authenticate the certificate automatically and hence cannot authenticate the sender's digital signature without human intervention. Thus, such a digital signature can give a false sense of security.

Email encryption is a preventive control to preserve confidentiality. Because the email program is not specific to any application, email encryption is a general control. The relevant security processes are authentication and authorization.

Person in the Middle Attack

This is a risk in sharing public keys. In the above example, Frank and Gail share their public keys by going through the corporate PKI. This is safe. But if Frank and Gail work in organizations that don't have PKI, they may send their public keys in plain text email. That's risky. The plain text public key can be intercepted by a hacker and replaced with the hacker's public key. By doing so, the hacker can intercept all subsequent encrypted email messages between Frank and Gail. Here is what can happen.

1. Frank sends his public key to Gail by email and vice versa.
2. Hank the hacker intercepts both emails and replaces the public keys with his.
3. Frank sends an encrypted email to Gail asking "will you marry me?" Frank encrypts the email using what he thinks is Gail's public key.

4. Hank intercepts the email and decrypts the email using his private key because Frank was actually using Hank's public key that Frank thought was Gail's.
5. Hank reencrypts the email using Gail's public key, which Hank has earlier intercepted and kept.
6. Gail is thrilled and sends back a quick reply, encrypted using what she thinks is Frank's public key (but it is actually Hank's), saying "sure!"
7. Hank intercepts the email and decrypts it using his private key because the email was actually encrypted using Hank's public key.
8. Hank changes the email to say "not a chance!".
9. Hank reencrypts the message with Frank's public key, which Hank has earlier intercepted and kept.
10. Frank is depressed and calls in sick for a week.

A PKI will mitigate this risk because public keys are centrally managed and authenticated. If two parties want to exchange public keys directly, the keys should not be sent in plain text email.

Secure Electronic Transaction

This is an eBusiness encryption protocol that hides the credit card number from the merchant and the order details from the credit card issuing financial institution to preserve privacy. It requires a customer to be issued a digital certificate by the financial institution. This increases the cost of the credit card issuing financial institution and decreases the portability of the customer because the customer then always has to use the same computer for eBusiness or has to install the digital certificate on any other computer where the customer wants to do eBusiness using the same credit card. Secure Electronic Transaction (SET) serves to reduce credit card fraud. A common cause of credit card fraud is weak security in merchants' servers. SET addresses the risk of merchants leaking credit card numbers because their servers are hacked. Under SET, the credit card number goes through the merchant site straight to the bank without being read by the merchant's server and therefore not kept in a merchant's systems. However, SET is not popular because of the high overhead on financial institutions and inconvenience to customers. It is not widely used in North America.

This is how SET works.

1. A customer receives a "personal" digital certificate from the credit card issuing financial institution. The certificate has the cardholder's private and public keys assigned by the financial institution. The customer stores it on a client computer or USB memory disk. The financial institution should require the customer to protect the certificate with a passphrase, i.e., to use a passphrase to activate the certificate every time it is used.

2. When the customer buys something on a web site, s/he sends his or her digital certificate to the merchant, which sends a copy to the financial institution. S/he also downloads the merchant's and the financial institution's digital certificates.
3. The customer's browser hashes the purchase order and the credit card information separately to form two message digests.
4. The customer signs the message digests to form a composite digital signature.
5. The digital signature is sent to the merchant which in turn forwards a copy to the customer's financial institution.
6. The customer uses the merchant's public key to encrypt the purchase order and s/he uses the financial institution's public key to encrypt the credit card information. The merchant forwards the credit card information to the financial institution, along with the amount to be charged.
7. The merchant and the financial institution use the customer's public key to decrypt the digital signature. The merchant and the financial institution use their private keys to decrypt the purchase order and credit card information.
8. The merchant and the financial institution independently computes the message digests of the purchase order and credit card information respectively.
9. The independently computed message digests are then compared to the message digests in the decrypted digital signature.
10. Now the merchant and the financial institution/ePayment vendor have authenticated the purchase and credit card information separately and independently.
11. The merchant does not have the credit card information in plain text, and the financial institution does not have the purchase order (what is purchased)
institution or payment vendor does not have the purchase details except the final amount. The financial institution or payment vendor sends a code to the merchant to approve or decline the payment order.
12. This helps to prevent credit card disclosure to unauthorized parties as the merchant does not have it.

Payment Card Encryption

The following encryption activities take place in payment card transactions.

1. The PIN, card number and expiry date are hashed together and stored on the card chip. This is in addition to the plaintext storage of the card number and expiry date on the card strip. The latter is required in order to support point of sales terminal that does not accommodate chip technology and also as a backup in case the chip is somehow more readable (e.g., damaged by wear and tear)
2. The card issuing financial institution encrypts the card number and expiry date using a card specific key and then subtracts the newly created or changed PIN from the last 4 digits of the encrypted value, and stores the difference, called a PIN offset. The PIN is not stored anywhere.
3. A PIN is verified by the financial institution using the above calculation and comparing the calculated PIN offset with the stored PIN offset.

4. A hash of the card specific key is stored in the chip, which is used by the card issuing financial institution to authenticate the card before verifying the PIN.
5. For offline terminal, the terminal computes the same hash as that stored in the card in step 1 and compares to the hash value read from the card.
6. The card number and expiry date are encrypted using the card issuing financial institution's public key and then stored in the chip. When a card is used online, the encrypted card number and expiry date are transmitted.
7. Card numbers and PINs sent by a financial institution which did not issue the cards, to the issuing financial institutions are encrypted using a symmetric key shared between the two financial institutions.
8. The card downloads the terminal's digital certificate and verifies it using the issuer's (e.g., Visa's) public key. Each point of sale terminal has a digital certificate specific to the brand of card acceptable (e.g., Visa).
9. The card downloads the terminal specific Triple DES or AES 112-bit key encrypted with the terminal's private key, which the card decrypts with the terminal's public key.
10. For offline transactions, the card encrypts the PIN, card number and transaction data using the terminal symmetric key for transmission to the terminal.
11. For online transactions, the point-of-sale terminal downloads the card issuing financial institution's digital certificate signed by the issuer (e.g., Visa).
12. For online transactions with a terminal, the card encrypts the terminal ID, card number and transaction data using the issuing financial institution's public key and sends it to the financial institution.
13. The financial institution sends the approval or "decline" message to the card.
14. The card then shares the message with the terminal.
15. The card then reencrypts the result of the transaction, i.e., approved or declined, along with the transaction amount, terminal ID, using the terminal public key and stores the encrypted data package called a transaction certificate, in the card.
16. The uploading of offline point of sale transactions to the merchant's financial institution is encrypted using a terminal specific symmetric key which has been sent to the financial institution encrypted with the institution's public key.
17. The settlement of the transaction between the card issuing financial institution, the credit card ultimate issuer (e.g., Visa) and the merchant's financial institution is encrypted using unique symmetric keys between each pair of organizations.
18. For ATM transactions, the ATM generates a one time symmetric key and encrypts it using the financial institution's public key and sends it to the financial institution.
19. Data transmission for ATM transactions is encrypted with the one time symmetric key.
20. Data transmission between the ATM financial institution and the card issuing financial institution is encrypted using a shared symmetric key between the two institutions.

21. For eBanking transactions, SSL encryption is used just like eBusiness.
22. The 3 or 4 digit card verification value (CVV) on the back of a credit card is not stored anywhere. It is derived by encrypting the card number and expiry date using a key specific to each card kept by the issuing financial institution.
23. The completed transactions should be sent by the point of sale terminal to the company's data center encrypted using the data center's public key.

Wireless Network Encryption

Wireless transmission of confidential information should be protected with strong encryption. An insecure wireless connection exposes users to eavesdropping. Here are some examples:

1. Email can be intercepted to be read or changed.
2. A hacker who hijacks a session can replace a user's credential with false information that leads to the destination server rejecting the user's access attempts, thereby causing denial-of-service.
3. An unauthorized person can log on a wireless network that is not secure and use the resources including free connection to an ISP.

Wireless security standards are evolving in the Institute of Electrical and Electronic Engineers (IEEE) 802.11 series, with 802.11i being the latest practical standard. These standards mainly address encryption. This is because the main risk of wireless traffic is eavesdropping. The encryption protocol that meets 802.11i is Wifi Protected Access (WPA). Here's how it works.

1. A device authorized to access an access point (wireless router) is installed with the access point's ID, called a service set ID (SSID), a static 128 bit symmetric key and the encryption software.
2. The access point sends challenge response text to the client device (desktop, laptop or phone).
3. The device encrypts the challenge response text and the SSID and sends it to the access point.
4. The access point decrypts the text and SSID and compares to the plain text that it sent out earlier. If there is a match, the device is allowed connection.
5. The access point and the device generate a new 128 bit symmetric key for each packet exchanged. The packet keys are encrypted using the static key for each device.

More security conscious organizations have implemented WPA2 which accommodates the use of 256 symmetric keys. In addition to complying with 802.11i, an organization may want to augment security with public key authentication by installing digital certificates on access points and devices.

WPA2 mainly uses an advanced symmetric encryption algorithm that requires a key length of at least 128 bits for authentication and encryption, called Counter Mode with Cipher Block Code Message Authentication Protocol. The actual key used for message encryption is a derivative of the static authentication key, random values generated by the access point and the remote device, as well as the MAC addresses of the access point and the remote device.

Smart Phone Encryption

Messages transmitted using smart phones can be protected with encryption. For example, the Blackberry Enterprise Server (BES) model integrates the device with corporate email. It uses Triple DES or Advanced Encryption Standard to encrypt information between a Blackberry device and an enterprise server in a corporate customer. A different symmetric key is assigned to each Blackberry by the enterprise server. An enterprise server is operated by a corporate customer for its employees and customers and the organization can choose to change the symmetric key as often as possible without involving Blackberry.

Blackberry Messenger (BBM) emails are encrypted using a common key controlled by Blackberry for all Blackberry devices and are therefore less secure than BES emails. A user organization may choose to assign its own common BBM symmetric key for the organization, for BBM emails within the organization, which, effectively, is more secure than relying on the common BBM encryption key. However, internally encrypted BBM email is much less secure than BES email.

On June 16, 2014, Blackberry announced the release of BBM Protected, which encrypts each message with a different key. The message symmetric key is encrypted with a static symmetric key exchanged once only between two parties the first time they contact each other using BBM Protected. This meets the United States Federal Information Processing Standards for cryptography.

Other smart phones can also be connected to corporate email systems using other software such as Microsoft Exchange Active Sync, but encryption may be less consistently applied because the exchange server or user PC connected to the smart phone may not enforce encryption. Blackberry has made its BES software available to other phone operating systems for a fee.
Smart phones connected to web mail accounts use the SSL protocol just like using a smart phone to browse the Web.

Mobile Payments Encryption

Encryption is also used for mobile payments. For example, a smart phone containing an RFID can be used to wave at a reader like a small credit card terminal and send the credit card number and expiry date in an encrypted form to the reader within 20 cm. The technology used is called near field communication (NFC) which is about a decade old

but has only recently been adopted for mobile payment. The phone downloads the reader's public key and uses it to encrypt credit card data. The same process applies to a chipped credit or debit card. Customers should hesitate using NFC payments with strange, small and obscure retail outlets because they might not be trustworthy in handling credit card data.

Limit of Encryption

Encryption cannot prevent file deletion. Role-based access controls are important. Another limit is that it relies on the encryption key, so there must be a process for key recovery in the event the key or the associated pass phrase cannot be obtained either because of human memory lapse, accidental deletion, misplacement of a smart card holding the key, or the departure of the staff members holding the key or pass phrase.

Most encryption software tools include a feature for an encryption administrator to use a special key to obtain the "lost" key. Such a special key should be kept offline under joint custody.

How Encryption Works with Other Access Controls

Encryption is often used with other techniques. Examples include:
Encrypting a password hash
Requiring a strong password or pass phrase to protect an encryption key
Using a token or a smart card to activate an encryption key
Encrypting biometrics.

However, some other technologies can be limited because encryption is used. The purpose of encryption is to prevent unauthorized disclosure. That means encrypted data can be read only with the proper keys and algorithms. Encrypted data therefore may not be subject to full inspection by other security mechanisms like firewalls, anti-virus software and intrusion detection systems. To enable these mechanisms to function effectively, network traffic has to be decrypted before the business applications process the data. The point of decryption reflects a risk based trade-off between confidentiality and the need to weed out malicious traffic. Host or client based detection malware detection tools can subject encrypted data to full inspection, that is, inspecting the data after decryption but before processing on the host or client.

Disk Wiping

The growth of electronic information is increasing organizations' exposure to loss. Unlike paper documents where massive access can be quite conspicuous, a large quantity of confidential information can be scanned by unauthorized people without notice in

seconds. It is critical that users realize the importance of safeguarding information on computers. In this digital world, it is not enough to just tell users not to store confidential information electronically.

Many people think that deleting files and even emptying the recycle bin will permanently remove the files. Computer forensic specialists have proved that files can be recovered even after a disk has been reformatted. It is therefore crucial for an organization to adopt a fool proof tool for disk wiping and enforce its use. Such a tool should be applied to computers that are reassigned, sold, donated or returned to the lessor. A popular product is Tabernus. Applying it five times will render data unrecoverable by even forensic data recovery programs. Similar data removal tools should be applied to smart phones.

Disk wiping prevents the unintended disclosure of confidential information. It can be applied at a general or an application level depending on the scope of the disk. The relevant security process is authorization.

File Blocking

Anti-virus software is never current no matter how frequently it is updated. This is because a vendor knows about a virus only after the virus has surfaced. To address the window of exposure created by new viruses that are not yet included in anti-virus software, organizations should adopt a practice of blocking executable (program) files in channels like email and downloading. A virus is a program, that's why blocking program files can help to guard against new viruses.

Very few employees have a need to receive programs by email. Most employees don't even need to download programs. An organization can block such file attachments and downloading, based on common file extensions such as .exe., .vbs., .com.

File Integrity Monitoring

We often check our work files using Windows Explorer and review the date of last change to ensure we are using the up-to-date files, e.g., when writing reports. In a corporate network, the high volume of files makes it impractical for someone to check for changes. Organizations should use tools to frequently check sensitive files for changes. This technique is similar to source code comparison discussed in Chapter Three. Because of the large file sizes, most large organizations can use hashing to check for file changes. You may recall from discussion above that a minor change to a file will change the hash, and that the size of a hash is much smaller than that of the source file. Thus, by hashing files in different time frames and comparing the hashes, an organization can find out whether a file has been changed and if there is change, the organization should seek the audit trail to support it. A good application is to check for changes to web site content to detect minor but critical changes made by a hacker. Another application is to check operating system files to detect rootkits.

File integrity monitoring is a detective control. It can be applied at a general or application level depending on the scope. It addresses the security objective of integrity and covers the process of monitoring.

Firewall

A firewall is a device used to protect a network from other networks. Any organization that hosts a web site, i.e., that exposes its network to the Internet, should have a firewall. Large organizations typically have many networks deployed horizontally and vertically. Horizontal deployment means putting firewalls at Internet entry points and vertical deployment achieves defence in depth by placing firewalls behind each Internet entry point at multiple layers.

A firewall's main function is to screen data traffic and the result of screening is either to accept the data or block it. It can be applied to both incoming and outgoing traffic, although the risk of incoming data is obviously higher.

A firewall screens data traffic basically using rules. Each rule will say what is allowed or what is to be rejected. A firewall can be configured to accept all traffic unless otherwise stated, in which case the rules are rejection rules. If the firewall is configured to reject all, the rules will be "allow" rules. Here is an example of an "allow" rule, that allows web surfing on the web server that bears the destination IP address, from anywhere.

Type	Source IP Range	Initiation Ports	Destination IP	Destination Ports
Allow	Any	80	142.107.93.143	80

Suppose the organization wants to block access from an IP range to the web server regardless of the type of access, it can implement the following firewall rule.

Type	Source IP Range	Initiation Ports	Destination IP	Destination Ports
Block	135,135.135.x	Any	142.107.93.143	Any

The above range includes IP addresses from 135.135.135.000 to 135.135.135.255, a total of 256 IP addresses under the current and gradually phased out IP address numbering scheme, IP v4. The number 256 equals 2^8, i.e., the last range of the number, each range consists of an 8-bit byte. Under the new IP address numbering scheme, IP v6, being phased in, this range would include 135.135.135.0 to 135.135.135.4294967295, i.e., 4,294,967,296 addresses.

A common hacking technique is IP spoofing, i.e., a hacker using an IP address of an innocent party. For example, a hacker may use an internal IP address of an organization to hack into the organization. An organization can mitigate this risk by blocking internal IP addresses from coming in. However, this has to be judicially applied. It is because a

bank employee is usually allowed to do eBanking from work. The firewall then, can block all incoming traffic bearing internal IP addresses where ports 80 and 443 are not used. Port 80 is used for web surfing and port 443 is used for encrypted web surfing including eBusiness. Another way to allow employees to use the Internet to perform banking transactions or purchase transactions with the employing organization is to route all such traffic within the intranet.

IP spoofing is also commonly used in distributed denial of service attacks (DDOS). The goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose - they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack. Denial of service attacks that use spoofing typically randomly choose addresses from the entire IP address space, though more sophisticated spoofing mechanisms might avoid unroutable addresses or unused portions of the IP address space. The proliferation of social media applications and connections makes DDOS easier and spoofing less important, but attackers typically have spoofing available as a tool, if they want to use it, so defenses against denial-of-service attacks that rely on the validity of the source IP address in attack packets might have trouble with spoofed packets. IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This type of attack is most effective where trust relationships exist between machines. For example, it is common on some corporate networks to have internal systems trust each other, so that users can log in without a username or password provided they are connecting from another machine on the internal network (and so must already be logged in). By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authentication.

IP spoofing is very difficult to prevent and detect because of the vastness of the Internet. One way is to obtain a list of unassigned IP addresses from IANA and throw that on the firewall. Instead of focusing on preventing or detecting IP spoofing in real time, organizations should expend their resources in preventing and detecting the effect of IP spoofing, i.e., large scale attacks, regardless of the legitimacy of the source addresses. However, when it is necessary to investigate the true sources for remedial actions or litigation, tracing can be done. This would require the cooperation of multiple ISPs and most likely law enforcement agencies.

There are basically three successively sophisticated ways a firewall can screen and block data: packet filtering, proxy and stateful inspection. These three methods can be applied cumulatively, i.e., a stateful inspection firewall can also use packet filtering and proxy filtering.

A firewall can be a router, an appliance with built in firewall software, a server with installed firewall software or simply a software tool installed on a PC. A PC firewall is also called a personal firewall. Personal firewalls can be freely downloaded from the Internet, but users should be cautious about the source, as the firewall may consist of a

virus. Large organizations should not use freely downloadable firewalls and should not let employees do that, by removing the local administer privilege of employees to their PCs, so they cannot install software.

A firewall prevents hacking. Because it applies to a network, it is a general control. The security assertion addressed is integrity and the relevant security processes are authorization and logging.

Packet Filtering Firewall

This firewall inspects every packet and compares the packet against a set of rules to determine whether the packet is acceptable. For example, a certain range of IP addresses can be programmed in a rule for rejection. The rules can be applied to each packet using "and" or "or". The firewall can also filter based on the MAC address (mainly for internal firewalls and wireless routers). Because a router operates on layer 3 of the Internet model, it is not capable of deciphering port numbers so it can usually be used only to filter IP addresses. A packet filtering firewall in the form of an appliance or server can inspect data at layer 4 and therefore also filter by port.

Proxy Firewall

A proxy firewall usually takes the form of a server with firewall software installed. In addition to packet filtering, a proxy firewall can check for malicious software and hide the internal IP addresses. A proxy firewall appears to the public as an internal host server and it appears to internal users as an external site. A proxy firewall operates on layer 5, the application layer and hence is privileged to all data in a packet.

Here is how IP address hiding works. Say an organization subscribes to IP addresses 123.123.000.000 to 123.123.255.255, in total 256^2 IP addresses, or 65,536 IP addresses. The organization will name its proxy firewall with IP address of say, 123.123.0.1. All the internal IP addresses can be numbered from 10.3.0.0 to 10.3.255.255. The 10.x.x.x range of IP addresses has been reserved by ICANN for internal use. Any organization can use this internally and Internet service providers (ISPs) know that such a range is not valid as routable external addresses. When a proxy firewall is used, an organization actually does not have to assign externally IP addresses to its computers and instead, and it only has to assign internal IP addresses. However, the downside is that if the proxy firewall is not functioning, traffic will come to a halt because ISPs cannot understand internal IP addresses; so the usual method is to still assign external IP addresses to computers but use the proxy firewall to mask the external IP addresses as internal IP addresses. What is the point in even using internal IP addresses if the only IP address outsiders see is the firewall's? Well, the firewall has to know which computer to route traffic to.

Stateful Inspection Firewall

Both packet filtering and proxy firewalls use rules to screen data traffic. A stateful inspection firewall, also operating at Layer 5, inspects the entire series of packets for a message instead of each packet in isolation. This requires more computing power. Every packet inspected is checked for context within the message to see if the packet is suspicious or invalid. For example, the firewall can check whether a packet bears the same session ID as the current session in which the packet is trying to join to detect a hacker trying to inject data to an otherwise genuine eBusiness transaction. A session ID is an ID assigned by a web server to a user upon the user initiating connection with the server. It helps the web server keep track of user activities for problem solving, customer relationship management, and knowing what a user has requested so the requested information can be provided to the right user. A stateful inspection firewall can also check the relationship between components in a packet, e.g., checking the length of all packets for a session within a certain time slot for port 443 (eBusiness), or for port 25 (SMTP mail) to assess whether the traffic is legitimate; a session sending an usually large volume of data for a stock trading transaction or a Google search to the web server is suspicious. A stateful inspection firewall takes the form of a server or an appliance. An appliance is a security appliance that comes preloaded with software.

Personal Firewall

An increasing number of personal computer (PC) users are installing personal firewalls on their computers. This can be downloaded as freeware or purchased by an organization to be installed on workstations and laptops. Modern operating systems include this as an essential feature. A personal firewall operates at layer 5 so is privileged to all incoming data. It generally operates in a silent mode because an organization may not turn on all of the alert options so as not to confuse users and also to conserve resources and hence maintain a high level of system efficiency. A personal firewall is the last firewall gate because by now, the traffic has passed the network firewall(s).

Because a personal firewall affects only one computer, an organization has a lot of choice in terms of tailoring the configuration to computers that contain highly sensitive information and are of high risk.

Unified Threat Management

Security vendors have come up with unified threat management (UTM) devices that are sometimes called the next generation firewalls. An UTM appliance can include firewall protection, anti-virus, intrusion prevention and spam filtering. Another UTM function is to look for accepted SYN packets that have not been matched to an ACK packet from the source after a time out period; after that, the packet is dropped to free up the port space. This will stop denial of service attacks engineered using half-open packets.

A UTM device carries out real time log analysis. It typically includes the following functions:

- Data aggregation **:** Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

- Correlation **:** looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution

- Alerting: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.

- Dashboards**:** Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.

- Forensic analysis**:** The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

Critical Properties of Firewall

For a firewall to be effective, it should have the following characteristics.

1. It should not be remotely configurable. That is, the change in configuration and rules should be done on site to prevent the firewall from being abused by a hacker. In the event that remote administration is absolutely necessary, e.g., when the premises cannot be accessed, rigorous two factor authentication should be used. Two factor authentication means using something the user knows and something the user possesses; ATM is a simple example. The firewall should be configured to send alerts to management when it is remotely managed.

2. It should log all traffic and the log should be analyzed using data mining software to detect anomaly.

3. The log should be monitored to avoid being full.

4. A firewall should be configured to fail close. That is, if for any reason, the firewall fails, e.g., the log is full, no traffic can go through. A firewall should be configured to deny all traffic by default, i.e., only the traffic that satisfies a rule is allowed.

5. After the first rule of global allow or global deny, rules should be put in to reject or allow based on criteria. A global deny rule will still admit traffic if there is a subsequent "allow" rule. Traffic that meets the "allow" conditions will be admitted. Similarly, rules that follow the global allow rule will determine what traffic will be admitted or denied. An organization that places a global deny rule will save time and be more secure in defining what is allowed. It is also an inherently safer approach than global deny. In global deny, if the organization omits a deny rule which is needed, malicious traffic will flow through.

6. After the global rule, rules will be exercised sequentially; so rule placement has to be careful, especially for deny rules. For example, after the global rule, if the next rule is to deny all access from IP addressed in a certain country, all such access will be denied even if there is a later rule to admit email traffic from that country. This is because a deny rule after the global rule will essentially drop the traffic. The same does not hold true for an "accept" rule, because accepted traffic does not go pass the firewall immediately, it is subject to further rules. This means the more rules there are, the slower the network will be; so it is important to periodically review firewall rules and remove unneeded ones.

   Here is an example.
   - A general rule to deny all is put in place.
   - A more specific rule allows access from any IP address to any IP address as long as certain ports are used, e.g., port 80, port 25 (SMTP mail) or port 443.
   - A lower level specific rule can be put in place to block certain IP addresses.

7. Firewall rules should be subject to the change control procedures that are discussed in Chapter Three.

8. A log retention schedule should be approved by management and audited periodically for effective compliance. Firewall logs are analyzed by intrusion detection systems. They are also used in forensic investigations.

Firewall Placement

Theoretically, a firewall should be placed on the outermost edge of an organization's network. However, it is often impractical to do all of the screening at that outward network point in order to avoid unnecessary performance degradation of the network.

A large organization should have multiple layers of firewall. This approach is called defence in depth. In addition, an organization needs to deploy at least one firewall at each network entry point; that is, installing firewalls horizontally. It is not unusual for a large organization to have tens of firewalls installed vertically and horizontally. While it is easier to understand the need for horizontal firewall placement, the vertical placement, i.e., defence in depth, warrants more discussion. Here is an example.

A bank may place a packet filtering firewall in front of each web server or a cluster of horizontal web servers. We say a cluster because seldom is one web server enough to handle all the incoming web traffic, so a cluster is used for load balancing and redundancy. Behind the web servers, the bank can place another layer of firewalls to inspect traffic before the application servers are accessed.

The rules in the external firewalls are less rigorous than those in the inner firewalls. This is because the web server should not contain confidential information. The rules will be targeted more at preventing denial of service attacks, defacement and change of critical information like posted interest rates.

When a transaction request needs to get past the web server, e.g., an eBanking transaction, the web server will direct the request to an authentication server to authenticate the customer. The transaction is then subject to screening by an internal firewall, which has more rigorous rules and most likely is more advanced, e.g., a proxy firewall. The area between an external firewall and the first internal firewall is called a demilitarized zone (DMZ). In traditional military terms, a DMZ is the frontier between two countries where military activity is not permitted. It is not as safe as homeland.

The common network devices situated in the DMZ are web servers, external email servers and external domain name servers. An external email server takes Internet email into the organization and vice versa. Because of the high volume of external network traffic, placing the external email server in the DMZ will lessen the traffic congestion in the interior network. Further, this server is also a common attack target. Although the server should be rigorously configured to prevent attack and is behind a packet filtering firewall, when it is attacked, the effect is somewhat limited because the internal network is not compromised. The worst result of such an attack is the organization's inability to receive or send Internet email temporarily. Although email messages could be compromised, an organization can install anti-virus software and use encryption to protect messages.

A web server is typically in the DMZ for the same reason as placing an external email server in the DMZ. The web server is a common target of attack and it should be kept away from the internal network to protect homeland. At the same time, there should be reasonable protection, by means of placing it behind a packet filtering firewall.

An external DNS translates deep URLs to local IP addresses. Because the deep URL is received from an ISP without full IP address resolution, the external DNS has to be placed at the network perimeter, i.e., the DMZ. It cannot be in front of the web server because the latter is the first server to receive incoming data traffic.

Honeypot

An organization may install a server that appears to process business transactions but does not. It is usually placed right behind the DMZ to attract hackers. The organization can use this server to capture hacker activities and analyze and learn from them to strengthen its security.

Intrusion Detection System

A firewall is critical to blocking malicious web traffic. It is not fool proof. Highly skilled and determined hackers will craft attacks that look very much like legitimate requests or transactions. For example, a hacker may piggyback on a web transaction and once inside the network, the extra code will generate widespread attack. This is where an intrusion detection system (IDS) is useful to mitigate the risk.

An IDS inspects data traffic that has passed firewalls and checks for anomaly. An anomaly is usually determined in aggregate, e.g., studying the pattern of traffic over a period and comparing the pattern to a base that has been built up and determined to be normal. A common anomaly is a surge is traffic from a range of IP addresses. Even though every session satisfies all the firewall rules for acceptance, the overall pattern is concerning. When an IDS determines an anomaly, it sends an alert to a security analyst, who will assess the alert based on established procedures. The procedures may call for escalation to management, collaborating with trading partners, IT service providers or security agencies as well as taking actions to block the traffic by placing a rule on the exterior firewall etc. Similar to a firewall, an IDS can use rules or mathematical modelling to identify anomalies. For example, if a worm attack is going around in the community, a rule can be placed on an IDS to look for a packet of certain size and of a certain sequence (similar to a virus signature) that arrives in a high frequency. An IDS that uses mathematical modelling is similar to stateful inspection firewall blocking; it studies traffic pattern and measures it against a baseline to detect rogue traffic. The baseline should be updated over time. This is also somewhat similar to a neural network that learns from doing.

An IDS can be placed on a network to scan all traffic that passes the network point or it can be connected to a server to inspect all traffic that has entered the server. The former is more economical while the latter can be more granular but is less timely because the traffic is already in the server. Organizations should use a mix of both. Certain highly sensitive servers should have their own IDS. An IDS should be placed at each critical juncture of the internal network. With respect to its relationship to horizontal firewalls, there might be an IDS for several horizontal network access points. An IDS addresses the security assertion of integrity and the relevant security process is authorization.

The rules (also called signatures) and criteria for anomaly determination should be updated regularly to prevent obsolescence that slows down data analysis and also to account for new threats. Software and security vendors send information about new

threats to their customers. Some IT research organizations also provide security alerts. One of them is SANS Institute in the United States. Organizations should be careful about interpreting security alerts from black hat sites which are hosted mainly for hackers. Although these sites provide some good information about security threats, there are sometimes hoaxes and the solutions may contain viruses.

Because malware is often used to steal information and launch attacks, modern IDS products have malware detection and forensic analysis functions. An example is FireEye. FireEye, Inc. is a global network security company that provides automated threat forensics and dynamic malware protection against advanced cyber threats, such as advanced persistent threats and spear phishing. Founded in 2004, the company is headquartered in Milpitas, California. The company's main product line consists of the Malware Protection System for web security, email security, file security, and malware analysis. The company has been involved with dismantling cybercriminal infrastructure.

In 2012, the company was named Silicon Valley's hottest security start-up, and was ranked the fourth fastest growing company in North America on the Deloitte 2012 Technology Fast 500.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

Intrusion Prevention System

An intrusion prevention system (IPS) is really a highly automated IDS. Some people call it an IDS on steroid. It can be configured to alert a security analyst to take preventive action or it might take the action automatically. An immediate action taken by IPS without the judgement of a security analyst is usually sending an instruction to the firewall administrator to put in a firewall rule to block further traffic of that nature, or if the IPS is connected to a firewall, to insert such a rule to the firewall directly. Some IPS have built in blocking capability.

Usually, the less urgent anomalies or rule infraction will cause an alert to the security analyst. Also, if the likelihood of false positive is high, the IPS should be configured to treat those scenarios by sending alerts to the security analyst to investigate before taking pre-emptive actions. A security analyst may have to contact the intruding organization to confirm whether the traffic is the result of an error, miscommunication, misunderstanding or an actual attack. There should be guidelines to help the security analyst, and to help that person to even decide whether to contact the "intruding" organization, as doing so may tip off the intruder. The incident response procedures we discussed in Chapter Three apply here. The procedures should address the need to document everything and make sure the audit trail is captured, which might be needed to investigate the incident and for forensic purpose. The criteria for escalation to different levels of management for decisions on network adjustment, new firewall rules to block traffic to fend off intrusion and forensic investigation should be clearly stated in the incident response procedures and such decisions and communications should be thoroughly documented. An IPS encompasses all the functions of an IDS. In addition, it has the ability to block traffic of the same pattern or anomaly. Most large organizations deploy a combination of IDS and IPS.

One might question the need for an IPS if the firewall is made stronger. Well, the rules and analysis performed at the firewall level cannot be too exhaustive, otherwise, it will slow down network traffic. The IPS will look at "iffy" scenarios and pattern. In other words, if a traffic stream (transaction) has a fairly high probability of being malicious, say more than 15%, it should be caught by a firewall. The rest is then left to the IPS. Firewalls and IPS slow down traffic because packets have to pass them to go further. Firewalls are placed in front of IPS when the latter is used because firewall rules are simpler and more definitive hence using less computing time and serve the purpose of blocking highly suspicious data traffic. Because of the impact on network performance, IPS should be placed on network nodes in front of highly sensitive servers or in the servers themselves. IPS can block traffic without referring to firewalls as by the time the traffic is deemed questionable, it has already passed a firewall. An IPS addresses the security assertion of integrity and the relevant security process is authorization.

Lock

Physical facilities should be restricted with access cards. The access cards will unlock the door. In addition, sensitive equipment should be secured with robust locks that can be opened with smart cards or keys that cannot be duplicated without notifying the key manufacturer. Laptops should be issued with locks that will work when the laptops are docked or loose. There should be instructions given to laptop users to lock their laptops to fixtures while unattended, and organizations should periodically patrol for compliance. For a highly sensitive device or room, a lock that requires two keys or combinations should be deployed.

A lock prevents unauthorized access and can be a general control or an application control depending on the scope of deployment. The security assertions supported are integrity and availability.

Management and Independent Review

Organizations continue to empower employees and customers with technology to expedite transaction processing. This results in a shift of manual to automated controls. While expediting transaction processing by giving users automated tools and direct access, an organization can mitigate the resultant risk of unauthorized transactions by using technology to perform rigorous analysis to produce exception reports for management to review. The reviewer, in some cases, may not be the manager of the user being reviewed. That's acceptable if the reviewer is independent of the process being reviewed and knowledgeable about the process. Here are the common access controls that involve exception reporting as well as management and independent review.

- Review repeatedly unsuccessful access attempts to assess the extent of policy compliance and user education as well as the practicality of the access controls.
- Periodic review of access rights to confirm appropriateness.
- Pre-approval of user profile and access control list changes and then verify the implemented changes to the pre-approvals.
- Pre-approval of firewall rule changes and then verify the implemented changes to the pre-approvals.
- Network layout changes pre-approve and post-review.
- Review of access logs to identify anomaly.
- Review of security incidents to ensure correction plan is in place.
- Review of summarized intrusion detection and prevention system reports to ensure mitigation actions have taken place.
- Review of system administration event log, in the form of exception reports generated using software to let management know of suspicious system administrator activities.

Management and independent review can be a preventive or detective control depending on the timing of review. It addresses mainly the authorization phase of the security cycle and the integrity security criterion. It can be applied at an application or general level.

Other non-security related management review depends on access controls to prevent change to information that is subject to review, e.g., preventing a treasury analyst from changing electronic bank statement information to hide reconciling items.

Password

This preventive control to authenticate users is simple and inexpensive. Its strength depends on the length, complexity and frequency of change. A password should be the first line of authentication. For more sensitive systems, two-factor authentication or biometric should be used to replace or augment passwords. Two factor authentication means requiring the user to provide something specific that s/he knows and something specific that s/he possesses, e.g., ATM card and the PIN.

Aside from being too short or too static, the risk of a password being disclosed, which is a control risk, depends on whether the password is stored or transmitted in plain text. A system should not store or transmit passwords in plain text. Here's how passwords should be stored and transmitted to avoid unauthorized disclosure.

A password entered is hashed by the computer that receives the password. Every operating system has this function. The hashing algorithm for creating a message digest can be used for password hashing. MD5 is commonly used to hash passwords.

The hashing algorithm hashes a password to a fixed length regardless of the original length of the password. An example of a hash is d3ccf205c702f315aad3b435b51404ee. The original password may be much shorter than this value. Next time you enter the password, the operating system (e.g., Windows) will hash the password using the same algorithm and then compare the hash with the hash stored in the computer. If they match, you are in. As long as you have not changed your password and key it in correctly each time, the hashed value will match the hash that is in storage in the hard disk. Once you change your password, a new hash is calculated to replace the stored hash. Because hashing is one way, someone who locates your password in the hard disk will see only the hash. If that person thinks that is the plain text password, it won't work. That is, if an unauthorized person keys in the hash as your plain text password under your ID, the system will hash that to a different value and try to match it with the hash stored, the two will not match so access will be denied.

If the hashing algorithm converts every password to a fixed length hash value, what is the point of using long password? Well, let's bear in mind that the hash is irreversible. This means a hacker cannot derive the actual password from the hash. S/he has to try different plain text passwords to try to match to the hash. So the longer a password, the more permutations a hacker has to try.

What if you are accessing a remote system like eBusiness? The password should be hashed by the remote server. Well, if the server does not have your original (real) password, how can you retrieve your password if you forget it? You could retrieve it from your personal notes stored in a secure place. Failing that, the server won't be able to tell you what the password is. This is why the help desk standard practice is to first verify your identity by asking you some challenge questions like your mother's maiden name or the model of your first car, answers to which you have provided before and are registered in the system. After that, the help desk will reset your password and the system should require you to change that temporary password to one that you can remember and meets the organization's password standard. A good password is one that you can easily remember but is difficult to be guessed by others; it should be a secret.

Passwords should be sufficiently long but not so long that people will be tempted to write them down. They should be subject to syntax check for a combination of digits and letters. They should be changed regularly. Users should adopt different passwords for different systems. This alleviates the risk of exposing your records in all systems that you access when your password is compromised.

Important Password Characteristics

Here is a list of key characteristics of a reliable password.

- Initial passwords should be communicated to the user directly in person, by telephone or through an encrypted channel.
- The password owner, on first login, must change the initial password.
- A password should contain at least 8 characters.
- A password should contain at least a digit, an upper case letter and a lower case letter.
- Passwords must not include easily identifiable personal information about the owner; e.g., names of family members, pets, birthdays, anniversaries or hobbies.
- Passwords must not be any words, phrases or acronyms that are part of the broadly recognized culture in the organization, e.g., diversity.
- Passwords must not be the same as all or part of a user's login id, actual last or given names, or a common nickname.
- A mechanism should be in place to ensure that passwords are not reused within a number of cycles. For example, the last ten passwords cannot be reused.
- Vendor default passwords must be changed upon installation.

- Regular users should change their passwords at least every 90 days.
- System administrators must change their passwords at least every 30 days.
- Password changes should not involve the use of easily recognized patterns, e.g. changing "nflpool01" to "nflpool02".
- Documented procedures must be in place to mitigate risk in the event of password loss, change or emergency modification.
- Passwords must be changed immediately if they have been or are suspected to have been compromised.
- Passwords must not be displayed while being entered but must be represented on the screen by a special character such as an asterisk.
- The system should disable the user after a number of consecutively incorrect password entries, e.g., five. The user will then have to call the help desk for password reset.
- Passwords must be hashed.
- Passwords to be hashed in a server must be transmitted from the client to the server in encrypted form.

Most of the above rules can be enforced by computers. User education is also important. A question often asked by people is why a bank requires its employees to change passwords but does not impose that on customers. Most people think it is because a bank does not want to inconvenience customers. Well, that may be true to some extent. The main reason is that a customer's password allows the customer access to only his or her information, whereas an employee's password allows access to corporate or customer information. The accountability is different. Banks, however, should encourage customers to change their passwords frequently.

A password is a preventive control for authentication that supports the assertions of confidentiality, integrity and availability. It can be a general control or an application control depending on its scope.

Password Cracking

If passwords are stored in hash, how does a hacker steal a password and use it? Well, such a person will first capture the hashed passwords that s/he wants to use. Such capture can be done by accessing the computer that holds the passwords along with the user IDs or by sniffing unencrypted network traffic.

The hacker will now try to hash a number of values and then compare each hash to the hashed password that is being attempted for cracking. If there is a match, the hacker knows the real password. The hacker will use the same hashing algorithm as that used by the system in question. This is not difficult, as there are only a handful of commercially used algorithms. The hacker will also research to find out the organization's password policy with respect to length, syntax and case sensitivity. Now, the hacker will use the process of elimination as follows. It will be done with software. There are numerous password cracking software tools available as free software or for a nominal price.
The hacker will first hash the common names and words that satisfy the password policy and compare each hashed value to the hashed password. If s/he knows about the password owner, this task is easier. For example, the hacker can hash the names of the owner, his or her pets, friends, family members, street names, sports celebrities or words that describe hobbies.

If the above does not produce a match, the hacker can hash dictionary words. If that still does not work, the hacker will conduct a brute force attack. This means s/he will hash all the permutations of characters (with replacement) that satisfy the password policy and compare each hash to the hashed password. Eventually, there will be a match. But that eventuality may take so long that the hacker will give up, even though the process is automated. Or the process will take so long that the cracked password has been changed by the user.

A hacker does not have to compute the hashes for every cracking attempt. There are pre-computed tables of hash values in the public domain or available in password cracking software tools.

So how long does it take to crack a password? It depends on the length and complexity of the password? It also depends on the power and number of computers used. A high end password cracker run on a powerful PC can compute up to 2.8 billion hashes a second. There are 3,087,630,118,591,490 permutations of 8-character, case sensitive, alphanumeric passwords. This means that such a random password takes 153 hours to crack.

However, most users select passwords that are easy to remember and therefore also easy to crack than a random password. Who would use $%*9Mczz as a password? Studies have shown that a user selected eight-character alphanumeric, case sensitive password takes an average of 18 hours to crack. Note that the work can be distributed over many computers to further speed up the time to crack. Well, the above cracking time is slightly longer if the hacker does not know the organization's password policy. For example, without knowledge that a system requires a password length of 8 characters, the hacker will have to try all passwords from say, 6 to 8 characters.

Advanced password algorithms use a salt to complicate the hashing. The above analysis is based on unsalted password hashes. Here is how salting works.

1. A user creates a password.
2. The password algorithm generates a random bit string, called a salt.
3. The password algorithm applies the salt to the password to create a hash.
4. The salt is stored separately from the hashed password but linked to the user account.
5. When the user uses the password again, the system retrieves the salt and uses it to hash the password. The hash is then compared to the stored hashed password to authenticate the user.
6. Common salt lengths are 12, 48 and 128 bits. A 12 bit salt can, on average, increase the password cracking time by 2,000 times, assuming the hacker knows the length of the salt but cannot locate the salt. The salt generates different hash values for identical passwords. However, once created or changed, a password will always have the same hash because the salt for the password is then statically stored. Not only does a salt make cracking much harder, it reduces the risk implication of a user selecting the same password for different systems because the salt is then independently derived by each system.

Some have said that passwords are now more a deterrent than a strong access control against determined hackers. As computing power doubles annually, passwords are increasingly crackable. This is why more and more organizations are opting to use pass phrases instead of passwords. Pass phrases are longer and easier to remember; and it can often be meaningful and unique to the owner, i.e., easy to remember but hard to guess. An example of such a pass phrase is “My son will be a Supreme Court justice.”

A consolation factor to password cracking is that organizations can rely on other access controls to protect the server that contains password hashes, e.g., by hardening the server in terms of tightening the operating system parameters, patching the computer rigorously with security updates, putting servers behind firewalls, installing host based intrusion detection and prevention systems, educating users to compose hard-to-crack passwords, encrypting password hashes when the server is inactive, encrypting password transmission and enforcing password rules to prevent cyclical passwords. Further, salting, as described above, can increase the cracking time in thousand folds.

Patching

We discuss Internet worms earlier in this chapter. A worm is sent by a hacker using the power and speed of the Internet to infect computers to cause denial of service or to disable certain security features to make it easier to hack into the network. A worm exploits a vulnerability in an operating system or other system software like a database

management system. This is a backdoor. Once the vendor realizes a backdoor is left open, it will send out a patch to its customers to install. For example, Microsoft issues patches at least monthly.

There are software products used to test and install the patches. Such a product automates the installation across an organization's network so that, for example, a network with 50,000 computers can have a patch installed within a day. Time is of the essence as software vendors and user organizations race with hackers.

What if a computer is turned off when a patch is rolled out? Well, corporate networks should be configured such that at connection, the network will check the patch level of the user computer and install the patch if required. This is done before the computer accesses other sites so as to prevent worm infection. Patches should generally be tested before being rolled out unless a patch is intended to address a zero day exploit.

Patching prevents Internet worms and hacking. It is a general control as the process can be applied to the whole organization. It addresses the security cycle of monitoring and supports the security assertion of integrity and availability.

Personnel Security Screening

People form one of the five components of a system. Some have said that people are often the weakest link in the chain of information processing as they can make mistakes and may not be trustworthy. Many IT staff members handle sensitive information so rogue or dishonest employees can hurt an organization and its customers. It is an increasingly common control for organizations to conduct personnel security screening of new hires including a combination of criminal record check, driving record check and credit check, depending on the job function. Personnel security screening prevents the hiring of rogue employees and ethically questionable consultants. It is a general control because the same procedures apply regardless of where the employee or consultant works in the organization. The security assertions supported are confidentiality and integrity and the security cycle addressed is authorization.

Security Education

To extend our argument that people often constitute the weakest link in the chain, it is important that their behavior supports the organization's access controls. They have to be educated on what is right and what is wrong in terms of controlling the assets and information in their possession.

A large organization should have a security education program that consists of classroom courses, web based training, posters and email reminders. Courses should range from general security to specific topics tailored to different job functions. Security education should include the following mandatory training:

1. New staff training.
2. New manager training.
3. Annual security training for IT managers.
4. Training for IT employees to address system design, architecture, programming, testing and technology infrastructure (including operating system administration).
5. Business user training for user requirement composition to address security.
6. Training on new security policies, procedures and systems for technical IT people and technical IT managers.

Optional training that is current and fun should be offered on the organization's intranet including quizzes to encourage employees to keep up to date with the organization's security policies. Posters should be placed in high traffic public areas to remind staff about common security practices like keeping a clean desk, locking laptops, choosing passwords that are hard to guess and shredding sensitive documents. Shredders should be placed next to printers to facilitate the shredding of sensitive documents printed by mistake.

Security education prevents rogue behavior or inappropriate handling of information. It is a general control as the employees being trained may come from different departments. The security cycle addressed is authorization and the assertions include confidentiality, integrity and availability.

Single Sign-on

We all have passwords to manage. I have ten different passwords. Wouldn't it be nice if I could use the same password for everything. I don't mean using the same value for all passwords. I mean using a password that is connected to all the systems I access regularly and once I key in the password, I have access to all the systems for which I am permitted. Well, that is not possible because my employer is not my bank etc. Most of my passwords are for connection to systems hosted by my employer. Wouldn't it be nice if I could log on to a portal once and it then makes all the other systems available to me based on my access profile? Well, that is the trend.

A single sign-on (SSO) system also presents a single point of failure so the risks of unauthorized access and loss of availability go up. The authentication requirement must be stronger than that for a typical system. For example, if a user name and a password allows someone to access seven systems which formerly required different logons and have different levels of sensitivity, the authentication requirement for single sign-on should be based on the system with highest sensitivity, not an average of the former authentication requirements for the seven systems. This means, if the password lengths required formerly ranged from 6 characters to 12 characters, the new single sign-on password length should be at least 12 characters, may be even stronger. Why even stronger? It is because if someone compromises that password, s/he has access to all systems.

An organization that adopts single sign-on should use two-factor authentication. SSO is particularly suitable to government operation to let citizens access all the services they are entitled to and have registered for. Canadian, Scandinavian and the Hong Kong governments are progressive in this area.

SSO is a preventive general control. It address the security process of identification and authentication. The security objectives of confidentiality, availability and integrity are supported.

Spam Filtering

Spam is more than a nuisance and productivity distracter. It slows down the network and can lead to denial-of-service. An organization should install spam filtering software, which may be part of the anti-virus software package. Spam filtering is a preventive general control and addresses the security assertions of availability. The security cycle of authorization is covered.

Employees should be educated about how to recognize and deal with spams. A recent internal survey conducted by Justice Canada shows almost 2,000 staff members were conned into clicking on a phoney "phishing" link in their email, raising questions about the security of sensitive information. The department launched the mock scam in December 2013 as a security exercise, sending emails to 5,000 employees to test their ability to recognize cyber fraud. The emails looked like genuine communications from government or financial institutions, and contained a link to a fake website that was also made to look like the real thing.

Staff Termination or Transfer Checklist

Many organizations have experienced information compromise, system damage or sabotage by staff members who are terminated or who resign on ill accord. This is why it is becoming a common practice to terminate the access right of employees as soon as such a situation arises. Even in harmonious parting, it is critical that an employee’s access rights be terminated on a timely basis. In addition, IT assets should be reclaimed immediately. Every organization should have a checklist to help ensure this takes place and the checklist should be part of the exit process administered by the line manager and monitored by the human resources department. This checklist should also apply to staff transfers. Technology continues to improve management’s ability to keep track of IT assets assigned so that they can be recovered.

The staff termination and transfer security checklist prevents rogue behavior and asset loss and it is a general control. The security cycle covered is authorization and the security assertions are confidentiality and integrity.

Standard Operating System Configuration Image

The operating system provides the foundation for access controls. There are many ways to configure an operating system including the browser to make services available, constrain services and ration resources. Loose configuration can open the doors to hackers and network worms. It can also lead to the loss of audit trail. An organization should have a standard image of what parameters should be turned on and what options should be activated for every PC and server. All PCs and servers should be configured according to standard images and the images should be reviewed periodically. Exceptions require management approval. Servers and workstations, including connected laptops should be periodically scanned for compliance with the standard configuration image. Applying a rigorous standard image of the operating system is called "hardening".
Using a standard image prevents system vulnerabilities. This is a general control because the images should apply to all computers. The security assertion addressed is confidentiality and integrity and the security cycle is authorization. The standard image should specify what services and ports are open, the extent of logging and the password configuration (how long, how complicated and when change is required).

The standard image for a browser should include the security settings such as acceptance of mobile code like Active X and Java, acceptance of unsigned code, acceptance of cookies, checking for a web site's P3P compliance and activation of a popup blocker. The standard image of a browser is harder to control because a user can often change the settings. This risk can be addressed in the security policy to tell users what they should not change.

Two Factor Authentication

In our discussion of passwords earlier, we conclude that passwords are becoming less reliable against hackers. This is why organizations are increasingly implementing two factor authentication, which requires something the user knows and something the user possesses. A common example is ATM. A two factor authentication system can tolerate a weaker password like a PIN. Of course, the stronger of both factors the better security is achieved. There are two other common methods for two factor authentication.

A system may require a personal digital certificate to be installed in a user computer which is activated with a pass phrase. The certificate and the pass phrase are the two factors. Another method is to give users a token that looks like a memory stick and displays a pass code that changes every minute. The pass code is synchronized between the token and the authentication server. A user has to key in this dynamic pass code and a static password to gain entry to a system.

Two factor authentication can be a general control or an application control, depending on the scope of implementation. It prevents unauthorized access and supports the security objective of confidentiality, integrity and availability. It is commonly used in virtual private network explained below. An increasing number of banks in Asia and Europe require two factor authentication for eBanking.

User Profile

We have discussed access control lists earlier in this chapter as a preventive control to restrict the information and system functions a user can access. Another way to exercise such a restriction, often at a less granular level but also to supplement access control lists, is by putting parameters in a user profile or a group profile. A group profile is a profile that applies to a group of users, e.g., all the users in department X.

Here are the common parameters that can be set in a user profile.

- The environments that the user ID can access, e.g., development, test or production.
- Time of day, day of week and day of month on which access is allowed.
- The group that the user belongs to.
- Expiry date.
- Special privileges that can override access control lists in the system or environment; e.g., a system administrator privilege classification has total access to a server regardless of access control lists. This would include installing programs on the server or workstation in which the user has a special privilege, or the so called system administration right. An "auditor" classification can have read access to all files in a server. "Auditor" here does not just mean internal auditors or external auditors. It means someone charged with the responsibility to perform ongoing data checking.
- Password expiry date.
- Last password change date.

User profiles should be used along with access control lists to prevent inappropriate access. A user profile is a preventive application control and it addresses the security objectives of authentication and authorization. The reason this is an application control is that a user may have different profiles for different systems.

Virtual Private Network

An organization often finds it necessary or desirable to allow employees and contractors to access the organization's network as if they were within the premises. There are basically two ways to do this. One is to set up the systems that need to be accessed remotely as an eBusiness server and the user would access it just like an eBusiness site. Another way is to give the user blanket access to the network and the user then has the

same degree of access to system functions as if s/he were in the office. The former is easier to control and the risk is lower. For example, many organizations have set up a web based mail server to allow employees to access corporate email from remote sites. We have discussed the web based access method to specific systems under eBusiness encryption. The second method is called virtual private network (VPN).

An example of a VPN application is to allow employees to work at home in the event of a disaster or a major disruption to city traffic. The organization would give the employee VPN access instead of setting up a web server for each of the application for any of three reasons. First, the frequency and user base for accessing a specific application may be too low to web enable the application. Secondly, the application may be too old to be web enabled, thus an employee can access it once admitted to the VPN using non-Web software as if s/he were in the office. Thirdly, the employee may need to access a variety of applications concurrently; thus letting him or her into a VPN would be more expedient than requiring the employee to log onto different applications via a browser.

Because a VPN allows a user blanket access to the network as if s/he were in the office, a high level of authentication requirement is adopted. It should use two factor authentication. A VPN typically goes through the Internet, so the entire data stream should be encrypted. Such encryption is similar to eBusiness encryption.

VPN prevents unauthorized access. It is a general control because it merely lets the user into the network. Once admitted, the user is still subject to the application level authentication like a user ID and a password for each application to which the user has been authorized to access. The security objectives supported are confidentiality, integrity and availability.

Vulnerability Assessment

We talked about the importance of installing patches from software vendors to close security loopholes left open during software product launch or implementation. Sometimes a patch does not reach a new computer because the computer was not registered in the network when the patch was applied or because the patching for that computer failed while the network was disrupted. Also, a patch may be undone because of errors by system administrators or the malicious effect of a worm. Another scenario is that even if all the patches have been applied, a security hole has been created by a system administrator in error by changing a number of parameters or created by an application in error to activate certain powerful operating system features that are seldom needed. Organizations should periodically review the configurations of operating systems and other system software to identify vulnerabilities and close them. This can be done by manually reviewing the configurations in the system, using scanning software to analyze the configurations or by trying to hack into a system. All three methods can be engaged in a progressive manner. Trying to hack into a system with authorization is also called ethical hacking or penetration testing. Some security firms, including the Big Four accounting firms, offer penetration testing services.

Here are the common steps involved in penetration testing.

1. Obtain senior management approval.

2. Map the network, i.e., studying the network to identify entry points including IP addresses. One might argue that this does not simulate hacking because a hacker would not have this information. If the penetration tester wants to be more objective and to simulate an actual hack more closely, s/he may decide not to rely on internal documentation of the network and instead, use external scanning, Internet research and social engineering.

3. Probe the network by using automated commands like ping to find out what ports are open on each web server.

4. Use security scanning software to scan web server for loopholes, e.g., unpatched operating system.

5. Try to hack into a system to view confidential information. There are automated tools available on the Internet and within the hacker community.

6. Obtain system administrator IDs and passwords of servers.

7. Obtain firewall, IDS and IPS rules.

8. Inject a small amount of bogus traffic to test the firewall and intrusion prevention system. There are automated tools available on the Internet and within the hacker community.

9. Shows attempts and ability to cause denial-of-service attack, defacement or changing data.

10. Report deficiencies to management and make recommendations for improvements.

Vulnerability assessment should also be conducted on systems under development and systems in operations in the form of code review. This should be targeted at identifying code that opens back doors or fails to detect hacking attempts that compromise program functions like SQL injection or buffer overflow. From a security perspective, code that handles web entered data needs to be more closely reviewed.

Vulnerability assessment detects system software security weaknesses and it is a general control because it applies to the network. It can be an application control if applied to a specific transaction processing server. The security assertions addressed are confidentiality, integrity and availability. The security process covered is monitoring.

Web Filtering

The Internet can be abused by employees to watch movies, listen to music or even visit indecent web sites such as sites that display pornography. An organization should monitor the use of the Internet by employees and make employees aware that monitoring takes place. Inappropriate use can cause harassment, legal liability and productivity loss. Organizations should filter web traffic to prevent abuse. For example, web sites in the nature of social media, gambling, pornography, weaponry, hate and terrorism can be blocked. So should web sites that transmit a lot of video. Some organizations block Youtube and Facebook. During the Olympics and World Cup Soccer tournament, an employer may even want to block certain sports sites. A U. S. research firm conducted a survey about Internet usage in large corporations recently and found that about half of the usage was not for corporate purpose.

Most employers condone personal use of the Internet, just as they condone personal use of the office telephone. However, excessively personal use should not be tolerated. Excessive users can be identified with web traffic monitoring. Organizations should implement software tools to monitor web traffic by employers and also to block undesirable sites. Such tools usually block sites based on URLs, IP addresses and also content by recognizing and analyzing the text and graphics. A web filtering software tool is seldom fool proof. A pornographic site that transmits such material not too explicitly may escape detection. This is why it is also important to report on high frequency Internet users and ask the managers to justify.

In addition to site blocking, such a tool can report on the number of attempts to each category that have been blocked and the computers that generated the attempts so the organization can consider following up with the management of the employees using those computers. In addition, the tool can be configured to report on the extent of traffic by computer to sites that are allowed, e.g., stock trading sites.

Web filtering prevents unauthorized use of the Internet and it addresses the security criteria of integrity and availability. Integrity is relevant because an undesirable web site is more likely to contain worms that can infect the organization's network. Availability is relevant because excessively personal use can slow down the network. Another aspect of integrity is related to the organization's reputation and legal liability. Imagine the consequence of employees going to a child pornography site and the organization is seen to condone it; or the consequence of a lot of employees going to sites that facilitate the exchange of unlicensed software or music. Web filtering is a general control because it is not related to any particular business application. The security process covered is monitoring.

Web Site Refresh

In the early days of the Internet, a common way of hacking is to deface a web site. This is easily noticeable and a standard solution is to disconnect the web server and reload the content from a backup and offline computer. The vulnerability that allowed the defacement also has to be closed by patching or shutting down some services and ports. Instead of defacement, a hacker may change a small part of a web site that can have a significant effect, e.g., changing a posted interest rate on a bank web site. Organizations have learned that it is a good practice to reload the web content from an offline computer periodically, perhaps several times a day, to nullify any unauthorized change. The offline version must also be checked regularly for currency and correctness.

Web site refresh is a corrective general control and it covers the security cycle of monitoring.

Security Monitoring and Reporting

To assess the reliability of the above security controls, organizations should periodically benchmark with comparable organizations, perhaps through professional security associations like Information Security Forum, www.securityforum.org. Such a platform also allow organizations to share best practices and experience while preserving anonymity to the public. Periodic, perhaps quarterly, security reports should be provided to senior executives including the IT steering committee. Such reports should include the security performance measures like the following.

- Percentage of the organization's information systems budget devoted to information security.
- Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery.
- Percentage space of remote access points used to gain unauthorized access.
- Percentage of staff members who have received security training in the past year, categorized as general staff, management staff, IT staff etc.
- Number of major audit recommendations of a security nature reported vs implemented.
- Percentage of information systems that have conducted annual contingency plan testing.
- Percentage of users with access to shared accounts.
- Percentage of incidents reported within required time frame per applicable incident category.
- Percentage of incidents resolved within required time frame per applicable incident category.
- Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets.
- Percentage of vulnerabilities remedied within organizationally specified time frames.

- Percentage of system and service acquisition contracts that include security requirements and/or specifications.
- Percentage of mobile computers and devices that perform all cryptographic operations using organizationally specified cryptographic modules operating in approved modes of operations.
- Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated.
- Number of hacking attempts identified.
- Number of successful hacking attempts.
- Percentage of web surfing attempts blocked by the organization
- Numbers of successful web surfing attempts by category, e.g., pornography, gambling.
- Top Internet users.
- Number of system outages.
- Number of virus attacks and number of devices affected by category like workstation, servers etc.
- Number of password reset requests.
- Turnover in IT security staff members.

MANAGEMENT CHECKLIST

1. Appoint a chief information security officer reporting to the CIO.

2. Set up an information security committee as a subordinate committee to the IT steering committee. The chief information security officer should be the chair.

3. Develop an information security strategy that supports the IT strategy.

4. Perform annual security risk assessment of the organization to assess inherent risk, control risk and residual risk. This assessment should include security testing such as vulnerability assessment.

5. Ensure that access control assessment is part of the systems development methodology.

6. Establish an information security policy as a corporate umbrella for access controls.
7. Develop information security standards for each technology platform such as database management system, eBusiness and cryptography. These standards can be used by individual business units to develop tailored procedures.

8. Develop corporate information security procedures to ensure consistent handling of security threats and incidents.

9. Conduct security check for new hires to sensitive positions including consultants.

10. Establish a security education program to ensure awareness of security policies, standards and procedures. This program should require employees to take annual refresher courses within the organization, e.g., online courses.

11. If the organization hosts eBusiness, it should establish network security monitoring procedures and tools to monitor for hacking attempts and network worms.

12. Periodically monitor the Internet traffic generated by employees to prevent inappropriate use including excessive use for personal purpose.

13. Assess the cost effectiveness of each common access control like password, encryption, lock and firewall. The purpose is to determine whether the controls are accepted, complied with, effective and generate the intended risk mitigation. This can be done by surveying users, reviewing system configuration and testing.

CONCLUSION

Access controls should be implemented at a general level and an application level. Management should assess the inherent risks with respect to authorization, occurrence and timeliness and then design general access controls as much as practical. The remaining risk should be mitigated with application level access controls until the residual risk is tolerable.

Access controls are implemented mainly to address the authorization and occurrence criteria. From the perspective of an IT specialist, the three common access control objectives are confidentiality, integrity and availability. For auditors, these can be tied to authorization and occurrence. Each access control serves one of the following five roles: Identification, Authentication, Authorization, Logging and Monitoring. Access controls support organization controls by enforcing segregation of duties, they support software change control by restricting access to source and object codes, they also support management and independent controls by preventing changes to exception reports and audit trail.

SUMMARY OF MAIN POINTS

Access controls take the forms of policies, standards procedures, system configuration, management review, independent review, exception reporting, system screening, access control rules and systems tools like passwords. Here is a list of common access controls.

- Access card – identification and authentication, preventive.
- Access control list – authorization, preventive.
- Access log – logging, detective.
- Anti-virus software – authorization, preventive.
- Biometric – authentication, preventive.
- Boundary checking – authorization, preventive.
- Challenge response – authentication, preventive.
- Clean desk practice (policy) – authorization, preventive
- Compliance scanning – monitoring, detective.
- Digital certificate – authentication, preventive.
- Digital signature – authentication, preventive.
- Disabling unnecessary system software features – authorization, preventive.
- Disk wiping – authorization, preventive.
- Encryption – authorization, preventive.
- File blocking – authorization, preventive.
- File integrity monitoring – monitoring, detective.
- Firewall – authorization, preventive.
- Hashing – authorization, preventive.
- Honeypot – authorization, preventive.
- Information classification – authorization, preventive
- Incident response procedures – authorization, corrective.
- Intrusion detection system – authorization, detective.
- Intrusion prevention system- authorization, preventive.
- Lock – authorization, preventive.

- Management or independent review – monitoring, detective.
- Password – authentication, preventive.
- Patching – authorization, preventive.
- Personnel security screening – authorization, preventive.
- Security monitoring and reporting – authorization, corrective.
- Security education – authorization, preventive.
- Single sign-on – identification and authentication, preventive.
- Spam filtering – authorization, preventive.
- Staff termination or transfer checklist – authorization, preventive.
- Standard operating system configuration images – authorization and logging, preventive.
- Two factor authentication – authentication, preventive.
- User profile – authentication and authorization, preventive.
- Virtual private network – authentication and authorization, preventive.
- Vulnerability assessment – monitoring, detective.
- Web filtering – authorization, preventive.
- Web site refresh – authorization and monitoring, detective.

REVIEW QUESTIONS

1. What is the relationship between privacy and access control?
2. Who should the chief information security officer report to and why?
3. Why is email encryption not very commonly used?
4. What are the relationships between access controls and other internal controls?
5. Which technique is used both in a password control and a digital signature? How?

6. How is defence in depth achieved?

7. What is the difference between hashing and encryption?

8. Where should an intrusion detection system be placed in relation to a firewall and why?

9. How does encryption affect anti-virus software tools and what should an organization do to address the effect?

10. What security risk can materialize if a domain name server is compromised?

CASE – Alibaba

Alibaba Group is an eBusiness giant operating globally and headquartered in Hangzhou, south China. Its operation includes business-to-business (B2B) online web portals, online retail and payment services, a shopping search engine and data-centric cloud computing services. Its initial public offering took place on September 19, 2014 on New York Stock Exchange, at $68 per share, raising $25 billion and surpassing all previous IPOs in the world. Its market capitalization stands at $221 billion, making it the fifth largest technology stock in the world and bigger than Facebook, Oracle, Bank of America General Motors and HSBC. The IPO represented 15% of total stocks issued.

Before this IPO, Alibaba was initially listed in Hong Kong Stock Exchange in 2007 for US$1.5 billion, making it the world's biggest Internet IPO since Google's. The company was privatized in 2012 and went through significant financial restructuring.

The Group began in 1999 when Jack Ma, an English teacher by training, founded the web site Alibaba.com, a B2B portal to connect Chinese manufacturers with overseas buyers. Ma, who started Alibaba from his Hangzhou (south China) apartment in 1999 with $60,000, watched his net worth swell to $26.5 billion as the shares rose, according to the Bloomberg Billionaires Index. Alibaba's consumer-to-consumer (C2C) portal Taobao, similar to eBay, features nearly a billion products and is one of the 20 most-visited websites globally. Alibaba Group's sites account for over 60% of the parcels delivered in China.

Alipay, an online payment escrow service, accounts for roughly half of all online payment transactions within China. The vast majority of these payments occur using Alibaba services.

Alibaba.com

Alibaba.com Limited, the primary company of Alibaba Group, is the world's largest online business-to-business trading platform for small businesses.

Founded in Hangzhou in eastern China, Alibaba.com has three main services. The company's English language portal Alibaba.com handles sales between importers and exporters from more than 240 countries and regions. The Chinese portal 1688.com was developed for domestic business-to-business trade in China. In addition, Alibaba.com offers a transaction-based retail website, AliExpress.com, which allows smaller buyers to buy small quantities of goods at wholesale prices.

In 2013, 1688.com launched a direct channel that is responsible for $30 million in daily transaction value.

Taobao

Taobao Marketplace, or Taobao, is China's largest C2C online shopping platform. Founded in 2003, it offers a variety of products for retail sale. In October 2013 it was the third most visited web site in China, according to Alexa.com. Taobao's growth was attributed to offering free registration and commission-free transactions using a free third-party payment platform.

Advertising makes up 85 percent of the company's total revenue, allowing it to break even in 2009. On November 11, 2014, the Chinese version of shopping "Black Friday" (although it was not a Friday), sales amounting to US$1.2 billion were made through Taobao. This same day sale grew by 35% from 2013.

Tmall.com

Tmall.com was introduced in April 2008 as an online retail platform to complement the Taobao consumer-to-consumer portal and became a separate business in June 2011. As of October 2013 it was the eighth most visited web site in China, offering global brands to an increasingly affluent Chinese consumer base.

eTao

eTao.com was beta-launched by Taobao in October 2010 as a comparison shopping website, and became a separate business in June 2011. It offers search results from most Chinese online shopping platforms,[1] including product searches, sales and coupon searches. Online shoppers can use the site to compare prices from different sellers and identify products to buy. According to the Alibaba Group web site, eTao offers products from Amazon China, Gome, Nike China and Vancl, as well as Taobao and Tmall.

Alipay

Launched in 2004, Alipay.com is a third-party online payment platform with no transaction fees. According to analyst research report, Alipay has the biggest market share in China with 300 million users and control of just under half of China's online payment market in February 2014. According to Credit Suisse, the total value of online transactions in China grew from an insignificant size in 2008 to around US$660 billion in 2012.

Alipay provides an escrow service, in which consumers can verify whether they are happy with goods they have bought before releasing money to the seller. This service was offered for what the company says are China's weak consumer protection laws, which have reduced consumer confidence in C2C and even B2C quality control.

The company says Alipay operates with more than 65 financial institutions including Visa and Mastercard, to provide payment services for Taobao and Tmall as well as more than 460,000 Chinese businesses. Internationally, more than 300 worldwide merchants use Alipay to sell directly to consumers in China. It currently supports transactions in 12 foreign currencies.

Alibaba Cloud Computing

Alibaba Cloud Computing (www.aliyun.com) aims to build a cloud computing service platform, including e-commerce data mining e-commerce data processing, and data customization. It was established in September 2009 in conjunction with the 10th anniversary of Alibaba Group.

AliExpress

Launched in 2010, AliExpress.com is an online retail service made up of mostly small sellers offering products to online buyers. The site has registered users and buyers in more than 220 countries.

Laiwang

In October 2013, the company's chairman Jack Ma announced that the company would no longer use WeChat and would henceforth promote its own messaging application and service, Laiwang.

ChinaVision Media Group

In March 2014, Alibaba agreed to acquire a controlling stake in ChinaVision Media Group for $804 million. The two firms announced they would establish a strategic committee for potential future opportunities in online entertainment and other media areas.

Company History

The company was founded in Jack Ma's apartment. He said, "One day I was in San Francisco in a coffee shop, and I was thinking Alibaba is a good name. And then a waitress came, and I said do you know about Alibaba? And she said yes. I said what do you know about Alibaba, and she said 'Alibaba and 40 thieves'. And I said yes, this is the name! Then I went onto the street and found 30 people and asked them, 'Do you know Alibaba?' People from India, people from Germany, people from Tokyo and China… They all knew about Alibaba. Alibaba - open sesame. Alibaba is a kind, smart business person, and he helped the village. So…easy to spell, and globally known. Alibaba opens sesame for small- to medium-sized companies. We also registered the name Alimama, in case someone wants to marry us!"

Company Timeline

- In December 1998, Jack Ma and other 17 founders released their first online marketplace named "Alibaba Online".
- From 1999 to 2000, Alibaba Group raised a total of US$25 million from SoftBank, Goldman Sachs, Fidelity and some other institutions.
- In December 2001, Alibaba.com achieved profitability.
- In May 2003, Taobao was founded as a consumer e-commerce platform.
- In December 2004, Alipay, which started as a service on the Taobao platform, became a separate business.
- In October 2005, Alibaba sold a 43% stake to Yahoo and increased Softbank's ownership to close to 40%, to secure cash for expansion. Yahoo has since reduced its holding to 23% before the IPO and 16% afterwards. Yahoo was required, as part of the IPO agreement, to dispose of 7% of Alibaba before the IPO. After the IPO, Softbank still owns 32% of Alibaba.
- In April 2008, Taobao established Taobao Mall (tmall.com), a retail website, to complement its C2C marketplace.
- In September 2009, Alibaba Group established Alibaba Cloud Computing.
- In October 2010, Taobao beta-launched eTao as a shopping search engine.

- In June 2011, Alibaba Group reorganized Taobao into three separate companies: Taobao Marketplace, Taobao Mall (Tmall.com) and eTao.
- In July 2011, Alibaba Cloud Computing launched its first self-developed mobile operating system, Alivun OS over K-Touch Cloud Smartphone.
- In October 2013, Alibaba decided to list in the New York or NASDAQ instead of Hong Kong, which was its first choice. This is mainly because Hong Kong Stock Exchange does not allow companies that do not give shareholders "one share one vote) to list. Alibaba has set up a management team of 30 senior managers to nominate members to the board of directors and make major company decisions. Ordinary shareholders cannot elect directors. This, in a way, is similar to other technology companies like Baidu (China's popular search engine, NASDAQ listed, and Facebook, where there are two classes of stocks and one class has much more voting right.)
- In June 2014, Alibaba acquired the Chinese mobile internet firm UCWeb. The price of the purchase has not been disclosed but the company did claim that the acquisition creates the biggest merger in the history of China's internet sector.
- On September 9, 2014, the Company was listed in New York Stock Exchange for $68 per share. The oversubscription prompted company principals and the investment banks to sell more shares, leading to total IPO amounting to $25 billion. Softbank and Yahoo still own 32% and 16% of Alibaba respectively. However, these two largest shareholders have given Jack Ma a free hand to run the Company, mainly because of his track record in China. On November 4, 2014, Alibaba posted its first quarterly earnings release as a public company that beat analysts' forecast, with overall 54% sales growth and 1,000% mobile revenue increase. Quarterly profit was $0.45 per share. Today (June 16, 2015), the stock is traded at US$86 a share.
- On November 7, 2014, Canadian Prime Minister Stephen Harper met with Jack Ma in Hangzhou after attending a China-Canada business conference, as part of the Prime Minister's visit to China to be present in part of the Asia-Pacific Cooperative meeting held in Beijing. Mr. Harper voiced hope that the Internet could help Canadian small to medium enterprises tap the Chines market.

Variable Interest Entity

Some analysts have raised concern about Alibaba's listing using the variable interest entity (VIE) structure. Investors are not buying shares in Alibaba Group directly. Instead, they are issued shares of Alibaba Holdings Cayman Islands, a variable interest entity (VIE) linked to Alibaba Group. VIE is a term used by the United States Financial Accounting Standards Board to refer to an entity (the investee) in which the investor holds a controlling interest that is not based on the majority of voting rights. This means shareholders do not own the Alibaba Group assets. Rather, they are beneficial owners of the value the Group's income and conveyed value, as determined by the Board of Alibaba Group. The reason

for using a VIE for the listing is that the Chinese Government does not allow foreigners to have ownership in Internet companies. Other Chinese technology companies listed on NASDAQ, like Baidu, also uses the VIE structure. Some analysts think that Chinese laws do not specifically allow the VIE structure.

Required

1. What are Alibaba's strategic and operational risks?

2. What IT governance and IT security governance should Alibaba put in place?

RUNNING CASE - Blackberry

Develop a security plan for Blackberry's network operations centres.

MULTIPLE CHOICE QUESTIONS

1. Which of the following provides the strongest protection against hackers?
   A. Operating system patching
   B. Access control list
   C. Firewall
   D. Virtual private network

2. Which of the following would be the most appropriate task for a systems administrator to perform?
   A. Configure the operating system.
   B. Develop access control lists.
   C. Develop a checklist for operating system configuration.
   D. Set a password policy.

3. Which of the following is most likely to change with technology?
   A. Security standard
   B. Security procedure
   C. Security configuration
   D. Security training

4. Which of the following technologies would conflict with encryption the most?
   A. Virtual private network
   B. Digital certificate
   C. Anti-virus software
   D. Password

5. Which of the following is the most effective solution for preventing external users from modifying sensitive and classified information?
    A. Security standards
    B. Intrusion detection system
    C. Access logs
    D. Encryption

6. eBusiness encryption uses
    A. asymmetric keys
    B. symmetric keys.
    C. session keys only.
    D. asymmetric keys and symmetric keys.

7. When a firewall log is full, the firewall will:
    A. let all traffic through
    B. either let all traffic through or deny all traffic depending on its configuration.
    C. deny all traffic.
    D. simply stop logging without affecting traffic screening.

8. Which of the following best protects the authenticity of an electronic document?
    A. Encryption
    B. Digital certificate
    C. Digital signature
    D. Checksum

9. Which is the most appropriate inference from a penetration test that cannot get through the network?
    A. The network is fool-proof.
    B. The test is deficient.
    C. There is no bad news about the network.
    D. The network is commercially reliable.

10. Which of the following generates an SSL encryption key?
    A. Browser
    B. Web server
    C. ISP
    D. Database server

CHAPTER NINE – OPERATING SYSTEM SECURITY

Security is, I would say, our top priority because for all the exciting things you will be able to do with computers – organizing your lives, staying in touch with people, being creative – if we don't solve these security problems, then people will hold back.

- Bill Gates

An American model is suing Apple after she claims naked photos were stolen from her iCloud account months before the recent celebgate hack where resulted in nude photos of stars including Jennifer Lawrence and Kate Upton flooding the internet. Joy Corrigan, 20, claims she tried to warn Apple in early July after fearing her account had been hacked when nude photos of her mysteriously leaked online.

She says Apple told her she had been the victim of phishing and that she needed to change her password. Joy Corrigan, 20, is suing Apple after she claims naked photos were stolen from her iCloud account months before the recent celebgate hack where resulted in nude photos of stars flooding the internet

But just days later her account was hacked again and when she again contacted Apple, she was told the same thing. After naked photos of over 100 actresses, performers and even Olympic athletes were released by a user on anonymous web forum 4Chan on August 31, Apple contacted her and denied any responsibility.

Corrigan is now launching a class-action lawsuit against the tech giant because of its 'crappy security' and she's seeking other victims to join her in the lawsuit, reports. The victims included the Oscar-winning young actress Jennifer Lawrence, ex-Downton Abbey star Jessica Brown Findlay, Spiderman heroine Kirsten Dunst, busty supermodel Kate Upton and reality TV phenomenon Kim Kardashian.

Hacked? Apple has denied that a flaw in the 'Find My iPhone' function (left) of Apple's iCloud service (right) may have helped the anonymous hacker to steal nude photos of Jennifer Lawrence and '100 other celebrities'. A list of celebrity names published anonymously online mentioned scores more targets including actresses Kate Bosworth and Selena Gomez, singer Rihanna, British models Cara Delevingne and Kelly Brook, and TV presenter Cat Deeley.

One video - reportedly showed Brown Findlay, who played Downton's Lady Sybil, was watched more than a million times online within hours of being posted. The alleged hackers claimed to have stolen the photos and videos from Apple's iCloud - the global system that stores photos and videos recorded on iPhones and other Apple devices.

Apple strenuously denies any responsibility for the leaked images. After celebgate, the company issued a statement in which it insisted the leak was not due to a flaw in its iCloud or Find My iPhone systems but the result of the actions of hackers.

'After more than 40 hours of investigation, we have discovered that certain celebrity accounts were compromised by a very targeted attack on user names, passwords, and security questions, a practice that has become all too common on the internet,' the statement read. 'None of the cases we have investigated has resulted from any breach in any of Apple's systems including iCloud or Find my iPhone.' The statement added that the company was 'continuing to work with law enforcement to help identify the criminals involved.'

The FBI is now investigating the hack.

Source: Read more: http://www.dailymail.co.uk/news/article-2755967/Model-sues-Apple-celeb-photo-leak-saying-warned-TWICE-security-months-before.html#ixzz3DOioYsoy

(Accessed on September 15, 2014)

The access controls we discussed in the last chapter apply to pretty much all systems and infrastructure. In this chapter, we will go over operating system security and some other technical security techniques in more detail to help auditors in performing in depth security assessments. The material in this chapter is beyond the requirements of the syllabuses of Certified Public Accountant, Chartered Professional Accountant and Certified Information Systems Auditor.

Operating System Security

In each operating system platform, an organization should have standard configurations for desktop, laptop, server and smartphones. Exceptions should be approved by management. There should be less room for exceptions for client devices (non-servers) as they are not application specific. Common controls in a standard image include disabling certain ports and services removing the ability to update the system register. A common restriction is to take away a user's ability to install software by not giving the user local administration right.

The operating system must be subject to the following security properties.

1. The operating system must protect itself from users. User applications must not be able to gain control of or damage the operating system, causing it to stop or destroy data.

2. The operating system must protect users from each other. One user must not be able to access, destroy or corrupt the data or programs of another user.

3. The operating system must protect users from themselves. A user's application module must not be allowed to destroy or corrupt another module.

4. The operating system must be protected from itself. No operating system module must be able to damage another module.

5. The operating system must be protected from its environment. For example, in the event of power outage, the operating system must be able to shut down in an orderly manner.

Windows Security

The description of Windows security is based on Windows 7. Organizations should keep versions up to date as old versions may not be supported by Microsoft. Windows XP is no longer supported but many bank ATMs still use this version, hence presenting a risk.

Windows facilitates security configuration and alerts settings in the Action Center. The Action Center has the following security features.

1. It allows the user to schedule Windows updates so that updates will be downloaded and implemented automatically.

2. Internet options – we will discuss these under a separate heading.

3. Firewall configuration for the Windows firewall.

4. Full disk encryption using 128-bit Advanced Encryption Algorithm.

5. Microsoft Security Essential, which is the Windows anti-virus software.

6. Data Execution Prevention feature that prevents buffer overflow by marking certain memory pages intended for data as non-executable.

7. Protected Media Path to protect digital rights management through denying access to digitally righted material by unauthorized applications. This prevents the copying of programs.

8. Locking down users to prevent them from installing programs.

9. Defining user access rights as guest, folder owner, administrator (full access), and specific user (requiring a logon account), in Active Directory.

10. Defining access control lists for folders and files.

Windows Event Logs

Windows logs key activities in an event log. Event logs are special files that record significant events on your computer, such as when a user logs on to the computer or when a program encounters an error. Whenever these types of events occur, Windows records the event in an event log that you can read by using Event Viewer. Advanced users might find the details in event logs helpful when troubleshooting problems with Windows and other programs.

Event Viewer tracks information as follows.

- **Application (program) events.** Events are classified as *error*, *warning*, or *information*, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that is not necessarily significant, but might indicate a possible future problem. An information event describes the successful operation of a program, driver, or service. This includes commands exercised at the command line and the execution of Windows systems commands, such as those carried out by systems administrators. A driver is a system program kept within Windows to support a device like a printer. A service is a feature in Windows that performs certain system transactions; an example is remote procedure call, which accesses the operating system instructions of a remote computer like a server or a connected workstation.

- **Security-related events.** These events are called *audits* and are described as successful or failed depending on the event, such as whether a user trying to log on to Windows was successful.

- **Setup events.** These events include the set-up of user profiles, access control lists, connected devices, installed applications etc. In other words, the creation, deletion or change of any Windows resources, users and applications are recorded.

DirectAccess

DirectAccess is a feature in the Windows 8 and Windows Server 2012 operating systems that provides remote connectivity to users. It was introduced in the Windows 7 and Windows Server 2008 R2 operating systems but has been improved for Windows 8 and Windows Server 2012. DirectAccess is similar in concept to a traditional virtual private network (VPN) but has several advantages.

The biggest advantage is that DirectAccess connections are more transparent than a VPN connection. Whereas users typically initiate and close VPN connections manually, Windows operating systems automatically initiate and close DirectAccess connections. This transparency means that as soon as the user's device is connected to the Internet, the user is able to access resources on the organization's intranet without manually initiating the connection. The DirectAccess connection is initiated when the user logs on to Windows. This automatic connection works in a single or bilateral direction and allows network administrators to remotely manage the device. Organizations have to implement strong client logon credentials with challenge response questions to prevent unauthorized access because of the automatic connection to the corporate internal network through the Internet.

Internet Explorer Security Features

Internet Explorer security settings can be configured for each of four zones: Internet, intranet, trusted sites and restricted sites. Trusted sites are sites that the user has almost full trust, e.g., a trading partner's site. Restricted sits are sites that are trusted and also that are seldom used and these site, by nature of their service, can cause significant damage to the user's system. Most users should have no restricted sites activated. For each of the four zones, a user can set the security configuration. For each zone, a user can select the default level, which provides about medium security, or to customize the setting. A user without system administrator right, i.e., an ordinary user, can still change the Internet Explorer security setting.

If a user selects the custom option, s/he can further define one of three parameters for the following browsing features. The three parameters are enable, disable or prompt. The browsing features supported by the custom option are:

1. Run .NET Framework reliant components not signed with Authenticode. Running such software components presented by a web site carries a significant risk, which the user, in this case, has the option to always accept, always deny, or decide that when prompted. The last option allows the user to assess the reliability of the web site and the application being used and decide whether to accept the running of an unsigned .NET Framework reliant software component. The .NET Framework is a collection of software tools for Windows application development, allowing for programming language interoperability, i.e., a program can include instructions written in other programming languages. Authenticode is Microsoft's tool for software distributors to digitally sign the software and for browsers to verify the digital signatures. It is a high risk for a user to select the enable option for running

.NET Framework reliant components not signed with Authenticode. The security risk of .NET is somewhat mitigated by the fact that these components usually are run in the sandbox. The sandbox is an enclosed area in Windows that does not allow access to local files and input functions, it is like an operating system within the operating system.

2. Run .NET Framework reliant components signed with Authenticode. This type of software is safer because it is digitally signed.

3. Accepting or rejecting mobile code such as ActiveX control components. ActiveX control is a framework for writing reusable code. Users should configure the browser to not accept unsigned ActiveX components automatically. ActiveX components usually are not run in the sandbox and therefore riskier than .NET components.

4. Enabling or disabling popup blocker.

A user can also specify the privacy settings by selecting a range from high to low. High is the safest and most restrictive. These settings mainly affect cookies. Here is the list of options:

1. Save cookies from any site.

2. Block third party cookies from site that don't comply with P3P.

3. Block third party cookies that save information that can be used to contact you without your consent.

4. Block first party cookies that save information that can be used to contact you without your consent. (The user is the second party.)

5. Block cookies from any site that is not P3P compliant.

6. Block cookies from any site that saves information that can be used to contact you without your consent.

7. Block all cookies from any site. Existing persistent cookies, i.e., cookies already on your hard disk can still be read by the web sites that created them.

Unix Security

This open source operating system predated Windows. Unix provides a lot of flexibility to users and systems administrators in configuring security. Common versions of Unix includes Linux for PCs, HP-UX for HP servers, AIX for the IBM AS400 mid-range servers and Solaris for Sun servers. Unix has its own version of active directory.

Authentication

A main difference between Unix and other operating systems is the way passwords are managed.

1. Password hashes are hidden from users because no one has a need to read them. The authentication server, of course, has access. Unix separate the hash from the user account in different files. To link the two, the user account file has a pointer called a shadow that points to the file with the hash and the location of the hash. This places the hashes a step more removed from the account IDs and therefore more difficult to compromise.

2. A salt ranging from 48 to 128 bits is added to the password for hashing, depending on configuration, Twelve bits of this bit string are hashed to form the first two bytes of the password hash.

3. Unix is quite sensitive to special characters like ^, @ and # and may interpret them as commands. Users should be cautioned to avoid these characters in passwords.

Authorization

Unix uses the following simple convention for data resource access control. It allows a file or directory to be defined as readable, writable (including deletion) and executable by the owner, anyone in the owner's user group or anyone else. A typical access control list is rwxr_x__x. This means the owner can perform all three functions, a group member can read and execute and anyone else can only execute. Execution means being able to run the program or use the function. Well, don't you have to read the program to run it? Not really, when we use ATM, we don't get to read the object code. If the file or directory contains only non-executable data, like a document, the third byte for each user type is set to "-".

Logging

Unix provides a large number of log files that can be configured by the system administrator. The most widely used and versatile is syslog. Syslog provides messages indicating what actions are being done on what resources and by whom. It also indicates the priority of the message that requires system administrator action.

MAC OS X

OS X has the versatility of Unix and also the GUI looks and feels of Windows. The system commands in OS X are actually Unix commands. OS X has all the security features that Windows has. Its web browser is called Safari, which is used in Mac

desktops, Macbooks, iPad and iPhone. Safari has similar security features to Internet Explorer. OS X has its own version of active directory. It supports full disk encryption using a 256-bit key. OS X is increasingly synchronous with iOS.

IBM Z Series (mainframe) Servers

These servers used to be called mainframe computers because of their large size in memory and disk storage. As PC based servers grow in size, the fast computing that was once the monopoly of mainframes is now affordable using PC based servers. Although there is still some difference in speed and power between these two types of computers, the difference is becoming narrower and narrower.

However, the architecture is different between PC based servers and Z series servers, as is the data format at the operating system level. For data representation, PC based servers use American Standard Code for Information Exchange (ASCII), which is more user friendly. Z series servers use Extended Binary Coded Decimal Interchange Code (EBCDIC), which involves a larger character set and therefore can accommodate a keyboard with more special keys. It is less user friendly, i.e., the data representation is less English like. The operating system used in Z series servers is z/OS. Z/OS is viewed by some as a more secure system than Windows and Unix mainly because it is a less popular target for hackers. However, in closer analysis, z/OS has fewer security features than Windows and Unix because its predecessors, Multiple Virtual Storage and Virtual Memory, were developed before the Internet and therefore not fully designed to mitigate today's hacking risks.

Z/OS is highly capable in supporting real time networks. A main reason is that real time networks were used by large organizations like banks well before the Internet. This enabled organizations to operate real time transaction systems that were geographically dispersed many years before the Internet was commercialized. Within z/OS, Structured Network Architecture (SNA) provides the network architecture to connect terminals (including z/OS emulated PCs) to servers, including TCP/IP support. Z/OS supports PKI and SSL.

Another component of z/OS, Customer Information Control System (CICS), provides the software framework for programmers to develop online real time systems that process customer transactions, like banking transactions. It is not a programming language. CICS is somewhat similar to .NET but it is more "close", i.e., it is not a collection of tools, but rather, a software structure with commands for programmers to use and it is very rigid.

Z/OS also supports systems development and production batch jobs via its Time Sharing Option (TSO). TSO allows programmers to submit programs for execution. It provides a text editor for changing Job Control Language (JCL). JCL is the z/OS equivalent to

Windows commands like copy, regedit or ipconfigsys; these are operating system commands that can be input in free form at the command line prompt. JCL also provides an operating system log.

Z/OS native security is viewed by many to be acceptable for systems development and local processing but leaving quite a bit to be desired for real time transaction processing. It provides user profile restriction for developers and program files. It also provides file protection via passwords. Its access control list functions are less robust than those in Windows and Unix.

CICS provides additional security by restricting access from individual workstations. It also provides restriction of access by end users like bank customers but leaves passwords optional. CICS cannot protect resources from external access, i.e., access by parties or objects not defined within the scope of CICS implementation in the environment, e.g., hackers or a user from another application that does not use CICS or is not within the same CICS environment. In other words, CICS does not offer operating system level security.

A typical CICS user in a financial institution is a teller or an ATM, but not a bank customer. To CICS, a user is the workstation, ATM or the web server session ID that has been assigned to the customer at that moment. To address the security shortfall of CICS, IBM offers an external security manager called Resource Access Control Facility (RACF) as an optional add-on to z/OS. RACF sits on z/OS and can interface with CICS, TSO or the OS directly.

RACF

RACF can be installed in a distributed manner. For example, a provincial or state government can host a RACF environment in each ministry or department, with the provincial or state environment as the master control. Policies are implemented at the global environment with certain parameters changeable in local environments.

RACF provides user authentication, resource access control, security logging and audit reporting. It is much more granular than operating system security. For example, it makes available 254 security levels (labels) that can be assigned to each resource object. A label indicates the users or objects that can access a resource and how. A resource object may be a data table (file), a program, a workstation, an ATM or another network device. In addition, RACF allows the RACF administrator to set up user profiles that dictate user access privileges. Resource profiles can be discrete or generic. Similarly, user profiles can be individual or group. A generic profile is like a group profile. A discrete or individual profile overrides a generic or group file in the event of conflict. Similarly, a user profile overrides a resource profile where there is a conflict, e.g., a user profile with the user class of Special has full access to all data files irrespective of the resource profiles. A user may also be a program or a system function. For example, RACF can define what data the payroll “add” function has access to and the extent of access.

An organization can set a default access profile for all resources which can be overridden with specific access profiles. For example, the default profile may say that only the owner can change and delete and everyone can read. There is a risk in this because unless a

specific access profile is created for a sensitive data table, everyone can read it. This default profile is called universal access authority (UACC). If the RACF administrator does not specify a value for UACC, the system assigned value is NONE, which means no one has access; a very safe approach, but may be too inflexible.

RACF IDs can be revoked automatically by the system once certain parameters are met. A RACF administrator can also manually revoke a user ID. Revocation does not mean deletion. A revoked ID can be revived. Revival is manual and is done by a RACF administrator. Examples of conditions for revoking user IDs are password attempt failures, departure from or transfer within the organization, and system abuse.

In addition to resource and user profiles as well as the universal access authority setting, the RACF administrator can set global options for each installation or for local domains within an installation. In conflict, global installation options will override the local environment domain options. The options are mainly for authentication and audit trail. Also, in conflict, a user profile setting like password change interval overrides a global setting (whether local or truly global). Here is the list of common options:

- Activate auditing for access attempts by class.
- Activate auditing for security labels.
- Activate checking for previous passwords and password phrases.
- Activate or deactivate auditing of access attempts to RACF-protected resources based on installation-defined security levels.
- Control change intervals for passwords and pass phrases.
- Control mixed-case passwords.
- Establish password syntax rules.
- Gather and display RACF statistics.
- Limit unsuccessful attempts to access the system using incorrect passwords.
- Log RACF events.
- Protect devices.
- Require that all work entering the system, including users logging on and batch jobs, have a security label assigned.
- Warn of password expiry.

RACF is a policy repository system. When access is requested by a system as part of transaction processing or by a user as part of ad hoc batch job, z/OS enquires RACF for the access policies for the data resource and the user and then grants permission or deny it. It is z/OS that contains the engine for access granting and denial based on policy settings in RACF.

Password Salting

Windows allows users to configure a password policy with respect to length, syntax, number of allowable attempts and expiry date. A password is hashed to a 128-bit value. Windows uses salting only for offline authentication, mainly for laptops. Salting is performed for offline access because the user cannot be authenticated by a server. For example, someone who travels with a laptop might want to do some work at home or in a hotel. Without access to Active Directory, the person will be authenticated based on the password hash stored on the laptop. This is how offline authentication works.

1. A network user creates a password.
2. Windows hashes without a salt and stores the hash on the server.
3. Windows hashes with a salt using the full user name as the salt and stores the salted hash on the laptop or desktop.
4. When the user logs in online, the server hash is used.
5. When the user logs in offline, the laptop or desktop hash is used.

Unix separates the password hash from the user account in different files. To link the two, the user account file has a pointer called a shadow that points to the file with the hash and the location of the hash. This places the hash a step more removed from the account ID and therefore more difficult to compromise. Unix also salts passwords with a salt length ranging from 48 to 128 bits.

Cryptography Algorithms

The strength of encryption depends on the rigor of the algorithm, the key length and the security over the key storage and transmission. The importance of key length is easy to understand and an organization can select that as a parameter in the encryption support system. The methods of key storage and transmission are also controllable by the user organization. The encryption algorithm is less determinable by the user organization and usually is specified by the encryption software purchased by the organization. A cryptography algorithm may be symmetric or asymmetric. Each algorithm usually can accommodate several key lengths. The following algorithms are commonly used.

Advanced Encryption Standard

The Advanced Encryption Standard (AES) standard was established by the U.S. National Institute of Standards and Technology (NIST). It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different symmetric key lengths: 128, 192 and 256 bits. AES supersedes Data Encryption Standard (DES), which was published in 1977. AES is now used commonly worldwide.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Triple DES

Triple DES was derived from DES, which was developed by IBM. Both are symmetric algorithms. In general, Triple DES with three independent keys has a key length of 168 bits (three 56-bit keys). The first key is applied to encrypt. The second is used to decrypt the result from the first key. The third key is used to encrypt again. Obviously, the result of step 2 is not the same as the original plaintext. Because the second step is decryption, it compromised the combined key length so the effective key length is 112, not 168. NIST has indicated that Triple DES is effective until 2030.

International Data Encryption Algorithm

International Data Encryption Algorithm (IDEA) is commonly used in SSL. It operates on 64-bit blocks using a 128-bit key, and consists of a series of 8 rounds. Each round uses six 16-bit sub-keys. The first eight sub-keys are extracted directly from the key, with key 1 (main key) from the first round being the lower 16 bits; further groups of 8 keys are created by rotating the main key left 25 bits between each group of 8.

CAST-128

CAST-128 is a symmetric-key block cipher used in a number of products including the popular non-PKI Pretty Good Privacy. The algorithm was created in 1996 by Carlisle Adams and Stafford Tavares. Another member of the CAST family of ciphers, CAST-256 (a former AES candidate) was derived from CAST-128. According to some sources, the CAST name is based on the initials of its inventors, though the authors claimed that "the name should conjure up images of randomness". CAST-128 applies 16 rounds with a 64-bit block size and a 128 bit key. Although Entrust, a large North American certificate authority, holds a patent on the CAST design procedure, CAST-128 is available worldwide on a royalty-free basis for commercial and non-commercial uses.

RSA

This asymmetric algorithm was developed by Rivest, Shamir and Adelman of MIT. It is a popular PKI cipher. The asymmetry is based on the practical difficulty of factoring the product of two large prime numbers. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factor servers as the private key.

Diffie-Hellman

Diffie–Hellman is a specific method of encrypting symmetric keys. The scheme was published by Whitfield Diffie and Martin Hellman. This algorithm is also commonly used in PKI, more commonly used in SSL key exchange. It is slower than RSA so is used less than RSA in encryption of data transmission.

Elliptic Curve Cryptography

Public keys are also used in mobile devices. Elliptic curve cryptography (ECC) is widely used on smart cards and smart phones. ECC is suited for small devices because the algorithm, by combining plane geometry with algebra, can achieve strong encryption with smaller keys compared to traditional methods like RSA that primarily use algebraic factoring. Small keys are suitable to phones in order to save computational power, RAM and battery time. A 224-bit ECC key can achieve the same strength as a 2,048 bit RSA or Diffie-Hellman key. Blackberry holds the ECC patents.

Digital Signature Standard

The Digital Signature Standard (DSS) algorithm is designed for digital signature, but not for data encryption. It is commonly used for signing downloadable software and documents. It is not part of PKI. DSS is slower than RSA and Diffie-Hellman so it is not suitable to data encryption. A digital signature is the encrypted hash. A hash is typically much smaller than a document so a slower algorithm is acceptable.

SHA-2

SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 currently consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits.

SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values. The SHA-2 family of algorithms are patented in US 6829355. The United States has released the patent under a royalty-free license.

In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2.

HMAC

Hash Based Message Authentication Code (HMAC) is similar to digital signature. However, it does not use asymmetric keys. Instead, a symmetric key is used. It is intended for secure exchange between two known parties. Because this is not intended for public communication, the key size can be smaller.

CMAC

Cipher Based Message Authentication Code (CMAC) is similar to HMAC except there is no hash. An encryption algorithm is used to encrypt the data and the encrypted text is truncated to a small value used for message authentication.

Mobile Device Security

Mobile devices are increasingly powerful and many people are shifting their reliance on laptops to smart phones and tablets for email and business transactions. One only has to take a subway ride to realize the extent to which people use smart phones to check email including business email. Lately, I am also seeing an increasing number of phones with credit card payment adaptors for accepting credit card payments. Just as people had concerns about Internet security when it blossomed, many are questioning the data protection when using smart phones and tablets for business. The security features of mobile operating systems and smart phones have matured in the last five years. We will discuss the common mobile operating systems security below.

iOS Security

The following are key security features in mobile devices running Apple iOS. The first six points were excerpted from an Apple white paper on iOS security, dated February 2014.

1. Touch ID is the fingerprint sensing system built into iPhone 5S, making secure access to the device faster and easier. To use Touch ID, users must set up iPhone 5S so that it requires a passcode to unlock the device. When Touch ID scans and recognizes an enrolled fingerprint, iPhone 5S unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it is still required under the following circumstances:
   - The phone has not been used for more than 48 hours.
   - After five unsuccessful attempts to match a finger.
   - When setting up or enrolling new fingers with Touch ID.

   Touch ID can be trained to recognize up to five different fingers. With one finger enrolled, the chance of a random match with someone else is 1 in 50,000.
   Touch ID can also be configured to approve purchases from the iTunes Store, the App Store, and the iBooks Store, so users don't have to enter an Apple ID password.

2. Encryption and Data Protection - The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused into the application processor during manufacturing. No software or firmware can read them. The UID is not recorded by Apple or its suppliers. The GID is common to all processors in a class of devices (for example, all devices using the Apple A7 chip), and is used as an additional level of protection when delivering system software during installation and restore. Integrating these keys into the silicon helps prevent them from being tampered with or bypassed, or accessed outside the AES engine.

3. The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if the memory chips are physically moved from one device to another, the files are inaccessible. The UID is not related to any other identifier on the device. Apart from the UID and GID, all other cryptographic keys are created by the system's random number generator.

4. Every time a file on the data partition is created, Apple's Data Protection creates a new 256-bit key and gives it to the hardware AES engine, which uses the key to encrypt the file.

5. By setting up a device passcode, the user automatically enables Data Protection. The passcode is "tangled" with the device's UID, so brute-force attempts must be performed on the device under attack. The stronger the user passcode is, the stronger the encryption key becomes. Users can choose to have the device automatically wiped if the passcode is entered incorrectly after 10 consecutive attempts.

6. Apple IDs are used to connect to a number of services including iCloud, FaceTime, and iMessage. To help users create strong passwords, all new accounts must contain the following password attributes:
   • At least eight characters
   • At least one letter
   • At least one uppercase letter
   • At least one number
   • No more than three consecutive identical characters
   • Not the same as the account name.

7. Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background. This behavior is achieved by using asymmetric elliptic curve cryptography.

8. iOS supports Exchange ActiveSyn to deliver email from Exchange servers to iPhones encrypted and vice versa.

9. iOS also supports the reading and sending of encrypted Outlook mail if the user installs the sender's digital and the user's private key.

10. iOS supports SSL.

Android Security

The Android platform takes advantage of the Linux user-based protection as a means of identifying and isolating application resources. The Android system assigns a unique user ID (UID) to each Android application and runs it as that user in a separate process. This approach is different from other operating systems (including the traditional Linux configuration), where multiple applications run with the same user permissions.

This sets up a kernel-level Application Sandbox. Applications cannot interact with each other and applications have limited access to the operating system. If application A tries to do something malicious like reading application B's data or dial the phone without permission (which is a separate application), then the operating system protects against this because application A does not have the appropriate user privileges. The sandbox is simple, auditable, and based on decades-old UNIX-style user separation of processes and file permissions.

Since the Application Sandbox is in the kernel, this security model extends to native code and to operating system applications. All of the software above the kernel, including operating system libraries, application framework, application runtime, and all applications run within the Application Sandbox. On some platforms, developers are constrained to a specific development framework, set of application program interfaces (API), or language in order to enforce security. On Android, there are no restrictions on how an application can be written that are required to enforce security. An API is a program supplied by an operating system vendor to help application developers to write code that can use certain operating system functions. The functions being accessed are typically of a utility nature like file handling and storage management.

In some operating systems, memory corruption errors generally lead to completely compromising the security of the device. This is not the case in Android due to all applications and their resources being sandboxed at the OS level. A memory corruption error will only allow arbitrary code execution in the context of that particular application, with the permissions established by the operating system. The system partition contains Android's kernel as well as the operating system libraries, application runtime, application framework, and applications. This partition is set to read-only.

Android provides a set of cryptographic APIs for use by applications. These include implementations of standard and commonly used cryptographic primitives such as AES, RSA, DSA, SHA and SSL. Android 3.0 and later provides full files system encryption, so all user data can be encrypted in the kernel using AES128. The encryption key is derived from the user password, preventing unauthorized access to stored data without the user device password. To provide resistance against systematic password guessing attacks (e.g. "rainbow tables" or brute force), the password is combined with a random salt and hashed repeatedly with SHA1. To provide resistance against dictionary password guessing attacks, Android provides password complexity rules that can be set by the device administrator and enforced by the operating system.

Some capabilities are restricted by an intentional lack of APIs to the sensitive functionality, e.g. there is no Android API for directly manipulating the SIM card. Sensitive APIs are intended for use by trusted applications and protected through a security mechanism known as permissions. These protected APIs include:

- Camera functions
- Location data (GPS)
- Bluetooth functions

- Telephony functions
- SMS/MMS functions
- Network/data connections

These resources are only accessible through the operating system. To make use of the protected APIs on the device, an application must define the capabilities it needs in its manifest. When preparing to install an application, the system displays a dialog to the user that indicates the permissions requested and asks whether to continue the installation. If the user continues with the installation, the system accepts that the user has granted all of the requested permissions. The user cannot grant or deny individual permissions — the user must grant or deny all of the requested permissions as a block.

Within the device settings, users are able to view permissions for applications they have previously installed. Users can also turn off some functionality globally when they choose, such as disabling GPS, radio, or wifi.

Android supports Exchange ActiveSyn to deliver email from Exchange servers to smart phones and tablets encrypted and vice versa. It also supports the reading and sending of encrypted Outlook mail if the user installs the sender's digital and the user's private key. Android is SSL compatible.

(Most of the above was excerpted from https://source.android.com/devices/tech/security/, May 20, 2014.)

Blackberry Security

Security has been Blackberry's strength in the smart phone market. But the Company cannot afford to be satisfied, as it was with its captive smart phone market before iPhone came to scene. It was rumored that during the early stage of Blackberry 10 development, some RIM senior management members casually commented that any security intrusion on the competitor phones could help RIM win back some market share. While on surface, this might sound logical, it was somewhat a passive attitude.

Corporate email through the Blackberry Enterprise Server (BES) is encrypted with the Triple Digital Encryption Standard (DES) or Advanced Encryption Standard (AES) algorithm. These algorithms use symmetric keys, i.e., the same key is used to encrypt and decrypt. A different symmetric key is assigned to each Blackberry by the enterprise server. An enterprise server is operated by a corporate customer for its employees and customers and the organization can choose to change the symmetric key as often as possible without involving Blackberry Limited. Messages routed from a corporate BES via an ISP to a Blackberry NOC and then to a wireless carrier are encrypted. Decryption occurs only when the messages arrive at the Blackberry handsets. Triple DES encrypts data in 64 bit blocks and uses a key length of 168 bits, which is stronger than eBusiness encryption. AES uses 256 bit keys. It is up to the corporate customer to choose between these two methods. Military organizations use AES.

Blackberry Messenger (BBM) email is encrypted using a common key controlled by Blackberry for all Blackberry devices and therefore less secure than BES email. A user organization may choose to assign its own common BBM symmetric key for the organization, for BBM email within the organization, which, effectively, is more secure than relying on the common BBM encryption key. However, internally encrypted BBM email is much less secure than BES email.

Blackberry Internet Service, i.e., browsing, does not have encryption by default. Blackberry has stated the following in its Knowledge Base.
Email messages sent between the BlackBerry Internet Service and the BlackBerry Internet Service subscriber's BlackBerry smartphone are not encrypted. When transmitted over the wireless network, the email messages are subject to the existing or available network security model(s).
"Existing or available network security models" above refers generally to Secure Socket Layer (SSL) encryption that is equivalent to eBusiness encryption at the option of the web site.

Here is a list of the Blackberry 10 security features:

- Transmission between BES server and Internet service provider (ISP) is encrypted using Transport Layer Security (TLS) or Secure Socket Layer (SSL), which uses eBusiness graded symmetric 128-bit keys.

- BES transmission from the ISP to a Blackberry NOC is encrypted using an AES key specific to each BES server.

- Transmission between a Blackberry NOC and a wireless carrier is encrypted using TLS or SSL.

- Transmission between a wireless carrier and the handset is encrypted using AES.

- Wifi can be encrypted using the required method specified by the access point (wireless router).

- Virtual private network encryption is supported to enable a secure tunnel for employees to access corporate networks to perform work that they could normally do as if they were in the office.
- SSL encryption can be enabled on the handset to secure web mail, Outlook Web Access email (corporate email through a web enabled Microsoft Exchange Server) and eBusiness.

- Blackberry Balance creates separate partitions for personal and work data. Both partitions can be encrypted. BlackBerry Balance – Blackberry Balance is a new feature introduced in BlackBerry 10, enabling users to keep both personal data and office work data separated in its own spaces. Using Blackberry Enterprise Service 10, IT departments can allow users to set up work-spaces that

automatically install applications and email accounts. After completion, users can navigate between personal and work profiles, by swiping down on the apps page. All of the user's data is secured via 256-bit encryption, and any files created will stay within the profile partition.

- Remote pushing of wifi and virtual private network profiles.
- Remote device killing, pushing of system configuration and purging of data.
- Forced password.
- Detection of kernel damage.
- Allowing limited apps in the work partition and personal partition.
- Malware protection.

CONCLUSION

PC and PC based server security continues to be improved by their vendors. Recently made available features include full hard disk encryption, application firewall and integrated malicious software features including anti-virus. In security, the weakest link is people, including people's commitment to define strong policies and comply with policies. Organizations should have tight operating system images for desktops and servers across the enterprise to comply with their policies. User access rights should be limited to their job functions and users should not be given administrator privilege to their desktops and laptops. System administrators should be controlled with thorough reference check, criminal record check before hiring and periodically thereafter, rotation of duties among servers, limiting the servers they support, limiting their other duties and regular management review of the system logs using software products to turn system logs into meaningful management reports.

MANAGEMENT CHECKLIST

1. Require system administrator to use longer and more complicated passwords than ordinary users. Require them to change passwords more frequently.
2. Secure server rooms with two-factor authentication.
3. Periodically assess operating system security features and follow a plan to enable and configure them in accordance with risk assessment and the security policy.
4. Develop policies and standard images for operating system configuration.

5. Periodically scan operating system and security feature parameters for policy compliance.

6. Establish patching procedures and monitor for compliance.

7. Disable employee access to the administrator account in their PCs.

8. Perform periodic review of the Active Directory configuration for compliance with the security policy.

9. Establish procedures for full disk encryption key recovery.

10. Conduct an annual review of operating system security for each operating system platform and report on overall security policy compliance.

SUMMARY OF MAIN POINTS

1. Differences between operating systems in terms of access controls mainly have to do with authentication, authorization and logging.

2. Windows salts passwords for offline access. The user name is the salt.

3. Unix stores a 12-bit salt as the first two bytes of the hash. The entire salt ranges from 48 bits to 128 bits.

4. Unix uses a shadow file to point to the actual password hash, which is stored in a separate file. This reduces the risk of password cracking.

5. An operating system mainly logs the program events, security events and setup events.

6. Ordinary users without local administration privilege can change browser security and privacy settings. This means more monitoring and education are required.

7. Anti-virus software, firewall and full hard drive encryption now come standard in commercial PC operating systems.

8. Ordinary users should not be given local administration privilege so that they cannot install software.

9. Management should install software to decipher system logs to produce meaningful management reports.

10. Z/OS has weaker security than Windows and Unix because its predecessors, Multiple Virtual Storage and Virtual Memory, were developed well before the Internet and not designed to mitigate the risk of hacking. RACF should be installed to provide commercial grade security for Z series servers.

REVIEW QUESTIONS

1. What are the purpose and functions of Active Directory?
2. What is a common way to prevent users from installing unauthorized software?
3. What is the purpose of the shadow file?
4. What is the purpose of the sandbox?
5. What type of access does a Special user in RACF have?
6. What are the three types of events recorded in the Windows Log?
7. What is the function of the password salt and how long is the Unix salt?
8. What are the CICS security deficiencies?
9. What OS components does RACF interface with?
10. Where is the Windows salt stored?

CASE #1 – Data Center Security

The following is a list of audit findings on operating systems controls in a government. The auditee was the department of information technology (DIT).

DIT did not fully restrict the use of privileged access rights to individuals based on their job function. Unauthorized use of privileged access rights could compromise the integrity of unemployment data and deny its availability. Our review of privileged access rights disclosed:

a) DIT did not restrict the security administration privilege to only security administrators.
b) DIT did not restrict the operations support privilege to only those individuals responsible for system maintenance and operations. This privilege allows individuals to manage all files. This privilege also provides full access, such as read, copy, add, delete or modify to these same files.
c) DIT did not prohibit all users from having multiple incompatible privileged access rights.

DIT did not properly secure human resources (HR) data and operating system files. As a result, DIT could not ensure that confidential unemployment data and critical operating system files were protected from unauthorized access and use. Our review of access to the third party service provider's mainframe computer system disclosed:

a) DIT did not restrict access to data files. The default system access allows all users to read and copy confidential employer and employee data, such as employee name, data of birth, personal identification numbers number and wage earnings without DIT knowledge.

b) DIT granted its development staff, operations support staff and the third party service provider's staff unnecessary modify access to application data files. Modify access allows users to bypass established controls and make unauthorized changes to data.
c) DIT did not restrict access to operating system files. DIT granted its development staff, operations staff and the third party service provider's staff modify access to the operating system files. These files contain codes that define system operation and system security. Inappropriate access to operating system files could adversely affect the availability of information systems to users.

DIT had not established effective security administration and monitoring over the third party service provider's mainframe computer system. As a result, DIT could not ensure that it would detect the unauthorized use of privileged access circumventing security and controls. Our review of security administration and monitoring disclosed:

a) DIT assigned individuals primarily responsible for system development the incompatible duties of security administration. The security administration privilege allows administrators to manage user accounts and assign access to system resources. Without proper segregation of duties, there is a risk that these individuals could grant themselves or others inappropriate access.
b) DIT did not assign the responsibility for security monitoring to an individual independent of the security administrator function. Consequently, DIT cannot ensure that the system administrator is performing only appropriate and authorized activities. The security monitoring and security administrator functions are incompatible and should be performed by independent individuals.
c) DIT did not define the system administrator duties and authority in the security administrator's position descriptions. Without defined duties and authority, DIT cannot evaluate security administrators or establish accountability for the security of the third party service provider's mainframe computer system.
d) DIT did not ensure that security administrators were adequately trained to effectively perform their job responsibilities. The security administrator's position descriptions did not identify the necessary knowledge, skills and abilities needed to effectively perform security administrator duties. Without identifying the necessary knowledge, skills and abilities, DIT management cannot ensure that security administrators receive appropriate training.
e) DIT did not have a strategy to monitor the privileged access of system administrators. As a result, DIT cannot be assured that its monitoring practices will deter or detect misuse of privileged access.
f) DIT had not developed and implemented complete security reports to monitor the privileged access to all user accounts. In addition DIT had not developed and implemented policies and procedures for monitoring security on the mainframe computer system. Security reports should identify the critical security activities to be monitored, which user accounts will be monitored, as well as the process for using and maintaining security reports.

DIT did not fully develop and maintain complete security requirements for the mainframe security system. Consequently, DIT did not properly configure the security system and effectively protect critical system resources. Although DIT and the third party service provider have made recent efforts to document the security requirements and settings of the security system, our review of DIT's efforts disclosed:

a) DIT did not clearly define its security administration role and responsibility in these security requirements. The agreement with the third party service provider stipulated that the Company was responsible for security administration. However, our review of the security requirements and DIT's practices indicated that DIT had not assumed responsibility for security administration.

b) DIT had not established policy and procedures to administer the third party service provider's security system. As a result, significant aspects of the security requirements of privileged access, resource access management and segregation of duties were not well defined or were missing. Policy and procedures would provide direction to the security administrator and facilitate development of complete security requirements.

c) DIT did not sufficiently understand the functions of the security system or the strategy used to configure it. According to DIT, documentation that explained the Company's initial strategy to configure the mainframe security system had been missing for several years. Maintaining complete and accurate documentation will help ensure that DIT security administrators understand the strategy used to configure the system.

d) DIT did not ensure the appropriateness of detailed security requirements and settings used to configure the third party service provider's security system. DIT did not explicitly agree to most of the third party provider's recommended security settings that were placed into operation. Although DIT recently documented these security settings, DIT should evaluate the appropriateness of the settings, revise where necessary, and document its agreement with the third party service provider.

Required

1. For each finding, assess whether the solution requires system configuration, management review, policy change, procedure change, or a combination.

2. For each finding, recommend a solution. For each solution that requires system configuration, state the solution in the z/OS and Windows environments.

CASE #2 – Target

The biggest retail hack in U.S. history wasn't particularly inventive, nor did it appear destined for success. In the days prior to Thanksgiving 2013, someone installed malware in Target's (TGT) security and payments system designed to steal every credit card used

at the company's 1,797 U.S. stores. At the critical moment—when the Christmas gifts had been scanned and bagged and the cashier asked for a swipe - the malware would step in, capture the shopper's credit card number, and store it on a Target server commandeered by the hackers.

Six months earlier the company began installing a $1.6 million malware detection tool made by the computer security firm FireEye, whose customers also include the CIA and the Pentagon. Target had a team of security specialists in Bangalore, India to monitor its computers around the clock. If Bangalore noticed anything suspicious, Target's security operations center in Minneapolis would be notified.

On Nov. 30, the hackers had set their traps and had just one thing to do before starting the attack: plan the data's escape route. As they uploaded exfiltration malware to move stolen credit card numbers - first to staging points spread around the U.S. to cover their tracks, then into their computers in Russia - FireEye spotted them. Bangalore got alerts on the same day and also December 2, and flagged the security team in Minneapolis.

For some reason, Minneapolis didn't react to the sirens. In the next few days, 40 million credit card numbers, 70 million addresses, numerous phone numbers, and other pieces of personal information gushed out of Target's servers.

When asked to respond to a list of specific questions about the incident and the company's lack of an immediate response to it, Target issued an e-mail statement: "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience. While we are still in the midst of an ongoing investigation, we have already taken significant steps, including beginning the overhaul of our information security structure and the acceleration of our transition to chip-enabled cards. However, as the investigation is not complete, we don't believe it's constructive to engage in speculation without the benefit of the final analysis."

More than 90 lawsuits have been filed against Target by customers and banks for negligence and compensatory damages. That's on top of other costs, which analysts estimate could run into the billions. Target spent $61 million through Feb. 1 responding to the breach, according to its fourth-quarter report to investors. It set up a customer response operation, and in an effort to regain lost trust, the Company promised that consumers won't have to pay any fraudulent charges stemming from the breach. Target's profit for the holiday shopping period fell 46 percent from the same quarter the year before; the number of transactions suffered its biggest decline since the retailer began reporting the statistic in 2008.

The CIO resigned in March and the CEO announced his departure in May. On June 10, Target announced the appointment of Brad Maiorino to the new position of chief information security officer. He previously occupied the same position in General Motors.

Required

Prepare a six-month action plan Target's chief information security officer.

RUNNING CASE — BLACKBERRY

Compare the security features of Blackberry 10, iOS and Android.

MULTIPLE CHOICE QUESTIONS

1. Which operating system is RACF applicable to?
   A. Windows
   B. Unix
   C. z/OS
   D. Mac OS

2. A salted password is?
   A. easier to crack.
   B. less visible.
   C. harder to crack.
   D. encrypted.

3. Which of the following pairs is most closely related?
   A. Single sign-on (SSO) and access control list
   B. Single sign-on and two factor authentication
   C. RACF and Mac
   D. Salt and access control list

4. Which of the following is run in a sandbox?
   A. Active X
   B. RACF
   C. NET components
   D. SSO

5. Which operating system uses CICS?
   A. z/OS
   B. Windows
   C. Mac OS
   D. Unix

6. Which operating system uses password shadowing?
   A. z/OS
   B. Windows
   C. Mac OS
   D. Unix

7. Which Internet zone is the safest?
   A. Restricted
   B. Trust
   C. Internet
   D. Intranet

8. Which cookie will still work even with the highest Internet Explorer privacy setting?
   A. Persistent and being used
   B. All persistent
   C. Existing session
   D. Session cookies from trusted sites

9. What is the following is included in the Windows Action Center?
   A. WPA encryption
   B. 128-bit Advanced Encryption protocol
   C. Intrusion prevention system
   D. Intrusion detection system

10. Who would be a frequent user of TSO?
    A. Bank customer
    B. Programmer
    C. RACF administrator
    D. Database administrator

Chapter 10 – SysTrust and Payment Card Industry Control Assurance

The most important thing for a young man is to establish credit – a reputation and character. – John D. Rockefeller

Organizations continue to increase their reliance on information systems. Aside from traditional outsourcing, there are arrangements for trading partners to share information systems, and for affiliated organizations to share their systems. For example, a retail company that opens its inventory system to a supplier for automatic replenishment may be assured of the reliability of the supplier's supplier chain management system. Another example is the ERP hosted by Ontario Government Treasury Board Secretariat being used by all Ontario Government ministries. The ERP is subject to a SysTrust audit. As a result, there is increasing demand on organizations operating information systems to provide assurance to external stakeholders. In this chapter, we will discuss two common types of such assurance reports, other than those in an outsourcing agreement, which was discussed in the last chapter. The two types of non-outsourcing IT control assurance engagements we will discuss in this chapter are:

- SysTrust, and
- Payment Card Industry security assurance

The These two types of control assurance engagement are highly security related as that is the concern created by eBusiness. The Internet is the IT trend and the risks it presents has caused consumers and corporate system users to feel uneasy about system reliability. These two standards are more rigid than CSAE 3416 discussed in the last chapter in that the control objectives and procedures are prescribed within the standards instead of being developed by the service organization. This is because the audience for these two standards is more specific, i.e., specific user organizations.

The Trust Services Standard was developed to address consumer concern about eBusiness and the engagement type was called Web Trust. It was a trust seal that could be placed on a web site once the web site hosting company passes an internal control audit based on the standard, carried out by a large accounting firm. The standard was later applied to SysTrust. Web Trust has become unpopular because consumers are now used to eBusiness and companies have found that a Web Trust seal had not significantly helped them attract or retain customers.

SYSTRUST

An organization that hosts an information system used by business partners like suppliers, corporate customers or affiliates may be demanded to provide internal control assurance with respect to the system. To ensure that such an engagement provides consistent assurance from organization to organization, Chartered Professional Accountants (CPA) Canada and American Institute of Certified Public Accountants (AICPA) developed the trust services standard to guide this type of internal control assurance.

Under the trust service standard, this type of internal control assurance is called SysTrust. The trust service standard starts with defining the following five trust services principles:

Security – The system is protected against unauthorized access.

Availability – The system is available for operation and use as committed or agreed.

Processing integrity – System processing is complete, accurate, timely, valid and authorized.

These three principles are mandatory in order for a SysTrust report to be issued.

Confidentiality - Information designated as confidential is protected as committed or agreed.

Privacy – Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy policy and the applicable privacy legislation.

These two principles are optional.

These principles should be applied to the following areas:

a. *Policies* – The entity has defined and documented its policies relevant to the particular principle. The term *policies* as used here refers to written statements that communicate management's intent, objectives, requirements, responsibilities and standards for a particular subject.

b. *Communication* – The entity has communicated its defined policies to responsible parties and authorized users of the system.

c. *Procedures* – The entity has put in place operation procedures to achieve its objectives in accordance with its defined policies.

d. *Monitoring* – The entity monitors the system and takes action to maintain compliance with its defined policies.

Once a service organization has decided to go ahead with a SysTrust engagement, it will hire an accounting firm to perform such control assessment and testing. The accounting firm must be licensed by CPA Canada or AICPA to perform the SysTrust engagement. Usually, only large accounting firms are licensed. In Canada, there are ten accounting firms that are currently licensed. Accounting firms in other countries will get their licenses from CPA Canada or AICPA.

The Trust Services model was developed initially for an engagement type called Web Trust. In the early days of eBusiness, consumers had concerns about security and whether the merchants would deliver the goods upon payment. CICA and AICPA saw the need to come up with a control assurance standard for eBusiness merchants to comply with and obtain a Web Trust seal from an accounting firm to place on their web sites if they pass the control standards upon an independent audit. WebTrust is now out of favor because more consumers are used to eBusiness and knowledgeable about recognizing whether a site uses encryption by looking for the lock. On a smaller scale, some certificate authorities (CA) provide malicious software protection assurance by reviewing a site's controls against malicious software and if a site is deemed to have such protection, a CA will give the site a security seal for a fee, to be placed on the web site. An example is Verisign's Trust Seal.

SysTrust was actually "invented" after Web Trust but it is based on the same control principles. The criteria are more detailed because a system is more complicated than a web site. SysTrust is widely adopted in North America.

Drivers for SysTrust

When an organization wants independent assurance about a system hosted by another organization, the user organization(s) may ask for SysTrust assurance. Sometimes, the initiative is taken by the service organization. When the initiative is taken by the user organizations, it may be driven by the following concerns.

- Remoteness of user organizations.
- Potential conflict of interest between the service organization and a user organization
- System complexity
- Frequent system failure
- Frequent evidence of unauthorized access
- Loss of data integrity
- Serious maintenance problems

Internal Control Criteria

Within each principle, there are internal control criteria that must be met by the service organization by designing and operating internal control procedures, which may be automated or manual. An internal control criterion is similar to an internal control objective. Unlike a control assurance engagement under CSAE 3416 or SSAE 16, a SysTrust engagement has little flexibility in terms of the internal control criteria. That is, the criteria in the SysTrust model are mandatory unless a service organization can explain why they are inapplicable to the system being audited and the SysTrust auditor agrees, e.g., there is no use of the Internet. The SysTrust model also provides a long list of illustrative internal control procedures for each criterion which the service organization could adapt. The service organization can also develop its own control procedures to

address the criteria. To support each criterion, the service organization must document the internal control procedures and demonstrate their effectiveness at a point in time or during the specified period of at least six consecutive months, as chosen by the hosting organization. We have listed below the internal control criteria. For the first criterion, we have also listed the illustrative internal control procedures. The criteria are grouped by principle.

Security Principle and Supporting Criteria

The security principle refers to the protection of the system from unauthorized access, both logical and physical. Limiting access to the system helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or use, alteration, destruction, or disclosure of information. Key elements for the protection of the system include permitting authorized access based on relevant needs and preventing unauthorized access to the system in all other instances.

1.0 Policies: The entity defines and documents its policies for the security of its system.

1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.

Illustrative Controls:

- Written security policy, addressing both IT and physical security, has been approved by the IT standards committee and is implemented throughout the company.
- As part of the periodic risk assessment process, the security officer identifies changes to the IT risk assessment based on new applications and infrastructure, significant changes to applications and infrastructure, new environmental security risks, changes to regulations and standards, and changes to user requirements as identified in service level agreements and other documents. The security officer then updates the security policy based on the IT risk assessment.
- Changes to the IT security policy are approved by the IT standards committee prior to implementation.

1.2 The entity's security policies include, but may not be limited to, the following matters:

a) Identifying and documenting the security requirements of authorized users.
b) Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, as well as retention and destruction requirements.
c) Assessing risks periodically.
d) Preventing unauthorized access.

e) Adding users, modifying the access levels of existing users, and removing users who no longer need access.
f) Assigning responsibility and accountability for system security.
g) Assigning responsibility and accountability for system changes and maintenance.
h) Testing, evaluating, and authorizing system components before implementation.
i) Addressing how complaints and requests relating to security issues are resolved.
j) Identifying and mitigating security breaches and other incidents.
k) Providing for training and other resources to support its system security policies.
l) Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
m) Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service level agreements and other contractual requirements.
n) Providing for sharing information with third parties.

1.3 Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.

2.0 Communications: The entity communicates its defined system security policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity's system security policies as well as changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system security are communicated to management and users who will be affected.

3.0 Procedures: The entity has put in place operation procedures to achieve its documented system security objectives in accordance with its defined policies.

3.1 Procedures exist to
a) identify potential threats of disruption to systems operation that would impair system security commitments and,
b) assess the risks associated with the identified threats.

3.2 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:
a) Logical access security measures to restrict access to information resources not deemed to be public.
b) Identification and authentication of users.
c) Registration and authorization of users.
d) The process to make changes and updates to user profiles.
e) Distribution of output restricted to authorized users.
f) Restriction of access to offline storage, backup data, systems and media.
g) Restriction of access to system configuration, superuser functionality, master passwords, powerful utilities and security devices.

3.3 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media and other system components such as firewalls, routers and servers.

3.4 Procedures exist to protect against unauthorized access to system resources.

3.5 Procedures exist to protect against infection by computer viruses, malicious code and unauthorized software.

3.6 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

3.7 Procedures exist to identify, report and act upon system security breaches and other incidents.

3.8 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classification as necessary.

3.9 Procedures exist to provide that issues of non-compliance with security policies are promptly addressed and that corrective measure are taken on a timely basis.

3.10 Design, acquisition, implementation, configuration, modification and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.

3.11 Procedures exist to provide that personnel responsible for the design, development, implementation and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.

3.12 Procedures exist to maintain system components, including configuration consistent with the defined system security policies.

3.13 Procedures exist to provide that only authorized, tested and documented changes are made to the system.

3.14 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.

4.1 The entity's system security is periodically reviewed and compared with the defined system security policies.

4.2 There is a process to identify and address potential impairment to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.

4.3 Environmental, regulatory and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.

Availability Principle and Supporting Criteria

The availability principle refers to the accessibility to the system, products or services as advertised or committed by contract, service level or other agreements. It should be noted that this principle does not, in itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made by mutual agreement (contract) between the parties.

1.0 Policies: The entity defines and documents its policies for the availability of its system.

1.1 The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity's system availability policies include, but may not be limited to, the following matters:
(See criterion 1.2 under the Security Principle.)

1.3 Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, as well as changes and updates to those policies, are assigned.

2.0 Communication: The entity communicates the defined system availability policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity's system availability and related security policies as well as changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system availability and system security are communicated to management and users who will be affected.

3.0 Procedures: The entity has put in place operation procedures to achieve its documented system availability objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threat of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.

3.2 Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practical.

3.3 Procedures exist to provide for backup, offsite storage, restoration and disaster recovery consistent with the entity's defined system availability and related security policies.

3.4 Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.

3.5 Procedures exist to restrict logical access to the defined system including, but not limited, the following matters: (See criterion 3.2 under the Security Principle.)

3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media and other system components such as firewalls, routers and servers.

3.7 Procedures exist to protect against unauthorized access to system resources.

3.8 Procedures exist to protect against infection by computer viruses, malicious code and unauthorized software.

3.9 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

3.10 Procedures exist to identify, report and act upon system availability issues and related security breaches and other incidents.

3.11 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

3.12 Procedures exist to provide that issues of non-compliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.13 Design, acquisition, implementation, configuration, modification and management of infrastructure and software are consistent with defined system availability and related security policies.

3.14 Procedures exist to provide that personnel responsible for the design, development, implementation and operation of system affecting availability and security have the qualifications and resources to fulfill their responsibilities.

3.15 Procedures exist to maintain system components, including configuration consistent with the defined system availability and related security policies.

3.16 Procedures exist to provide that only authorized, tested and documented changes are made to the system.

3.17 Procedures exist to provide that emergency changes are documented and authorized.

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system availability policies.

4.1 The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.

4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.

4.3 Environmental, regulatory and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis, policies are updated for that assessment.

Processing Integrity Principle and Supporting Criteria

The processing Integrity principle refers to the completeness, accuracy, validity, timeliness and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner and free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions are processed or all services are performed without exception. Validity means that transactions and services are not processed more than once and that they are in accordance with business values and expectations. Accuracy means that key information associated with the submitted transaction remains accurate throughout the processing of the transaction and that the transaction or service is processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization means that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

1.0 Policies: The entity defines and documents its policies for the processing integrity of its system.

1.1 The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity's processing integrity policies include, but may not be limited to, the following security matters:
(See criterion 1.2 under the Security Principle.)

1.3 Responsibility and accountability for developing and maintaining the entity's system processing integrity and related system security policies, changes, updates and exceptions to those policies are assigned.

2.0 Communications: The entity communicates its documented system processing integrity policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

a) The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters:
   (i) Time frame for completion of transactions;
   (ii) Time frame and process for informing customers of exceptions to normal processing of orders or service requests.
   (iii) Normal method of delivery of goods or services, including customer options, where applicable.
   (iv) Payment terms, including customer options, if any.
   (v) Electronic settlement practices and related charges to customers.
   (vi) How customers may cancel recurring charges, if any.
   (vii) Product return policies and limited liability, where applicable.

b) Where customers can obtain warranty, repair services, and support related to the goods and services purchased on its web site.

c) Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.

2.2 The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.

2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.

3.0 Procedures: The entity has put in place operating procedures to achieve its documented system processing integrity objectives in accordance with its defined policies. (Procedures may be manual or automated.)

3.1 Procedures exist to (1) identify potential threats of disruption to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.

3.2 The procedures related to completeness, accuracy, timeliness and authorization of inputs are consistent with the documented system processing integrity policies.
If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters:

a) The entity checks each request or transaction for accuracy and completeness.
b) Positive acknowledgement is received from the customer before the transaction is processed.

3.3 The procedures related to completeness, accuracy, timeliness and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.
If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters:

a) The correct goods are shipped in the correct quantities in the time frame agreed upon, or services and information are provided to the customer as requested.
b) Transaction exceptions are promptly communicated to the customer.
c) Incoming messages are processed and delivered accurately and completely to the correct IP address.
d) Outgoing messages are processed and delivered accurately and completely to the service provider's (SP) Internet access point.
e) Messages remain intact while in transit within the confines of the SP's network.

3.4 The procedures related to completeness, accuracy, timeliness and authorization of outputs are consistent with the documented system processing integrity policies.
If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters:

a) The entity displays sales prices and all other costs and fees to the customer before processing the transaction.
b) Transactions are billed and electronically settled as agreed.
c) Billing or settlement errors are promptly corrected.

3.5 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.

Security related criteria relevant to the system's processing integrity

3.6 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:
(Refer to criterion 3.2 under Security.)

3.7 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers and servers.

3.8 Procedures exist to protect against unauthorized access to system resources.

3.9 Procedures exist to protect against infection by computer viruses, malicious code and unauthorized software.

3.10 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Criterion related to execution and incident management used to achieve objectives.

3.11 Procedures exist to identify, report and act upon system processing integrity and related security breaches and other incidents.

Criteria related to the system components used to achieve objectives.

3.12 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

3.13 Procedures exist to provide that issues of non-compliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.14 Design, acquisition, implementation, configuration, modification and management of infrastructure and software are consistent with defined processing integrity and related security policies.

3.15 Procedures exist to provide that personnel responsible for the design, development, implementation and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.

Change management related criteria applicable to the system's processing integrity.

3.16 Procedures exist to maintain system completeness, including configurations consistent with the defined system processing integrity and related security policies.

3.17 Procedures exist to provide that only authorized, tested and documented changes are made to the system.

3.18 Procedures exist to provide that emergency changes are documented and authorized.

3.19 Procedures exist to protect the system against potential risks that might impair system processing integrity.

3.20 Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity practices.

3.21 Procedures exist to provide for the completeness, accuracy and timeliness of backup data and systems.

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.

4.1 System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.

4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing, integrity and related security policies.

4.3 Environmental, regulatory and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.

Confidentiality Principles and Criteria

The confidentiality principle refers to the system's ability to protect the information designated as confidential, as committed or agreed. Unlike personal information, which is defined by regulation in a number of countries worldwide and subject to the privacy principles, there is no widely recognized definition of what constitutes confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is

available only to those who need to access to complete the transaction or to resolve any questions that may arise. To enhance business partner confidence, it is important that the business partner be informed about the entity's system and information confidentiality policies, procedures and practices. The entity needs to disclose its system and information confidentiality policies, procedures and practices relating to the manner in which it provides for authorized access to its system and users and shares information designated as confidential.

1.0 Policies: The entity defines and documents its policies related to the system protecting confidential information, as committed or agreed.

1.1 The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity's policies related to the system's protection of confidential information and security include, but are not limited to, the following matters:
(refer to criterion 1.2 under the Security Principle.)

1.3 Responsibility and accountability for developing and maintaining the entity's system confidentiality and related security policies, as well as changes and updates to those policies, are assigned.

2.0 Communications: The entity communicates its defined policies related to the system's protection of confidential information to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The system confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided.
This communication includes, but is not limited to, the following matters:

a) How information is designated as confidential and ceases to be confidential. This includes the handling, destruction, maintenance, storage, backup, distribution and transmission of confidential information.
b) How access to confidential information is authorized and how such authorization is rescinded.
c) How confidential information is used and shared.

d) If information is provided to third parties, disclosures including any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.
e) Practices to comply with applicable laws and regulations addressing confidentiality.

2.3 Responsibility and accountability for the entity's system confidentiality and related security policies as well as changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect confidentiality and system security are communicated to management and users who will be affected.

3.0 Procedures: The entity has put in place operation procedures to achieve its documented system confidentiality objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruption to system operation that would impair confidentiality commitments and (2) assess the risks associated with the identified threats.

3.2 The system procedures related to confidentiality of input, processing and output are consistent with the documented policies.

3.3 The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.

3.4 The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.

3.5 In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the system confidentiality practices in place when such information was received, or obtains customer consent to follow the new confidentiality practice with respect to the customer's confidential information.

System security related criteria relevant to confidentiality

3.6 Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters:
(Refer to criterion 3.2 under the Security Principle.)

3.7 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media and other system components such as firewalls, routers and servers.

3.8 Procedures exist to protect against unauthorized access to system resources.

3.9 Procedures exist to protect against infection by computer viruses, malicious code and unauthorized software.

3.10 Encryption or other equivalent security techniques are used to protect transmission of user authentication and other confidential information passed over the Internet or other public networks.

Criterion related to execution and incident management used to achieve the objectives

4.1 Procedures exist to identity, report and act upon system confidentiality and security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.12 Procedures exist to provide that system data is classified in accordance with the defined confidentiality and related security policies.

3.13 Procedures exist to provide that issues of non-compliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.14 Design, acquisition, implementation, configuration, modification, as well as management of infrastructure and software are consistent with defined confidentiality and related security policies.

3.15 Procedures exist to help ensure that personnel responsible for the design, development, implementation and operation of systems affecting confidentiality and security have the qualification and resources to fulfill their responsibilities.

3.16 Procedures exist to maintain system components, including configuration consistent with the defined system confidentiality and related policies.

3.17 Procedures exist to provide that only authorized, tested and documented changes are made to the system.

3.18 Procedures exist to provide that emergency changes are documented and authorized.

3.19 Procedures exist to provide that confidential information is protected during the system development, testing and change processes in accordance with defined system confidentiality and related security policies.

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.

4.1 The entity's system confidentiality and security performance is periodically reviewed and compared with the defined system confidentiality and related security policies.

4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its system confidentiality and related security policies.

4.3 Environmental, regulatory and technological changes are monitored, and their impact on system confidentiality and security is assessed on a timely basis. System confidentiality policies and procedures are updated for such changes as required.

Privacy Principle

The privacy principle focuses on protecting the personal information an organization may collect about its customers, employees and other individuals. Some personal information is considered sensitive. Laws and regulations in most developed countries define the following to be sensitive personal information:

- Date of birth
- Personal ID number like a social security or social insurance number
- Consumer purchase history
- Finance
- Medical or health condition
- Offence or criminal conviction
- Sexual preference
- Trade union membership

There are no privacy control criteria specified in the Trust Services Standard. We have discussed the privacy internal controls in Chapter Five. The Trust Services Standard contains generally accepted privacy principles, which are consistent with the privacy principles discussed in Chapter Five.

Disclosure Related to E-commerce Systems

For an e-commerce system, the organization has to make the following disclosures in connection with the Trust Services Principles. The respective control criteria in the related principles are quoted below, with an emphasis on disclosure.

Security and Availability

1. The security and availability obligation of users and the entity's security commitment to users are communicated to authorized individuals.

2. The process for informing the entity about breaches of system security and for submitting complaints is communicated to authorized users.

3. Changes that may affect system security are communicated to management and users who will be affected.

Processing Integrity

1. The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2. The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.

3. The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of system security and for submitting complaints is communicated to authorized users.

4. Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.

Confidentiality

1. The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.

2. Changes that may affect confidentiality and system security are communicated to management and users who will be affected.

Privacy

The organization must disclose its privacy policy and procedures to support the ten generally accepted privacy principles discussed in Chapter Five, including the contacts for obtaining access and complaints. The following information must be disclosed.

- Purpose of collection of personal information.
- What consent means and how it is given.
- How personal information will be used.
- Who personal information may be shared with.
- Security over personal information.
- Who to contact for questions, complaints and access to personal information.
- Privacy policy.

Process of a SysTrust Engagement

1. An organization hosting a system used by other organizations decides to secure a SysTrust opinion on the system's reliability. This is called the service organization.

2. The service organization prepares the system description to be consistent with the contract of service. The description should include infrastructure, software, procedures, people and information.

3. The service organization selects none, 1 or both of the 2 optional SysTrust principles to comply with, i.e., confidentiality and privacy.

4. The service organization reviews the SysTrust criteria and decides which ones do not apply. Provide justification for those that do not apply, e.g., the system is not connected to the Internet.

5. The service organization develops internal control procedures (manual and automated) to support each criterion, using the illustrative controls in the SysTrust model as guidance.

6. The service organization decides on whether the assurance sought will be at a point in time or for a period of 6 to 12 months.

7. The service organization hires a large accounting firm licensed by CPA Canada or AICPA to perform a SysTrust assurance engagement. The accounting firm is now called the service auditor.

8. The service auditor reviews the system description for consistency with the contract of service, and to assess its comprehensiveness and correctness.

9. If the service auditor has a significant concern about the system description, it should ask the service organization to correct. If the service organization does not address the concern to the accounting firm's satisfaction, the firm should withdraw from the engagement.

10. The service auditor reviews the list of control criteria excluded by the service organization and assesses the appropriateness of rationale. If the service auditor does not agree with the service organization and the latter does not address the disagreement to the service auditor's satisfaction, the service auditor should withdraw from the engagement unless the service organization decides to drop the relevant principle. If the criteria affected are part of confidentiality or privacy, the service auditor can continue with the engagement but agrees with the service organization to exclude such optional principles from the scope.

11. The service auditor reviews the internal control procedures (manual and automated) for each criterion and assesses their adequacy to address the criterion.

12. If the service auditor is not satisfied that a criterion is adequately supported by internal control procedures, it should raise with the service organization for correction. If the service organization cannot correct to the accounting firm's satisfaction, the service auditor should withdraw from the engagement, or make sure the service organization understands that the opinion will be qualified. Another option is for the service organization to exclude the relevant principle.

13. If the service auditor is satisfied that there are sufficient stated internal controls to support each criterion, the service auditor conducts control testing with the aim of achieving high assurance.

14. If a significant control deficiency is found, the service auditor presents to the client and informs the client that the control is not reliable. If the client does not correct the control retroactively and does not come up with a compensating control for the auditor to test, the service auditor will have to qualify the opinion, unless the control can be removed without impairing the reliability of the relevant criterion (i.e., the control is redundant), or unless the relevant principle is removed.

Sample System Description

The following is an illustrative system description suggested by CPA Canada and AICPA.

Background

XYZ Co. Pension Services (XPS), based in New York, New York, with offices across North America, manages and operates the Pension Administration System (PAS) on behalf of pension plan sponsors who are XPS's customers. The plan members are the employees of XPS's customers who are enrolled in the pension plan. XPS uses PAS for recordkeeping of pension-related activities.

Infrastructure

PAS uses a three-tier architecture, including proprietary client software, application servers, and database servers. Various peripheral devices, such as disk drives, and laser and impact printers, are also used.

Software

The PAS application was developed by programming staff in XYZ Co.'s Information Technology Department (XITD), Systems Development and Application Support area. PAS enables the processing of contributions to members' pension plans and withdrawals at retirement, based on plan rules. PAS generates all the required reports for members, plan sponsors, and tax authorities. PAS also provides a facility to record investments and related transactions (purchases, sales, dividends, interest, and other miscellaneous transactions). Batch processing of transactions is performed nightly. PAS provides a facility for online data input and report requests. In addition, PAS accepts input from plan sponsors in the form of digital or magnetic media or files transmitted via the telecommunications infrastructure.

People

XPS has a staff of approximately 200 employees organized in the following functional areas:

1. Pension administration includes a team of specialists that set up pension rules, maintain master files, process contributions to PAS, report to plan sponsors and members, and assist with inquiries from plan members.
2. Financial operations is responsible for processing withdrawals, depositing contributions, and investment accounting.
3. Trust accounting is responsible for bank reconciliation.
4. Investment services is responsible for processing purchases of stocks, bonds, certificates of deposits, and other financial instruments.

5. XITD has a staff of approximately 50 employees who are dedicated to PAS and its related infrastructure and are organized in the following functional areas:
   - The help desk provides technical assistance to users of PAS and other infrastructure as well as plan sponsors.
   - Systems development and application support provides application software development and testing for enhancements and modifications to PAS.
   - Product support specialists prepare documentation manuals and training material.
   - Quality assurance monitors compliance with standards and manages and controls the change migration process.
   - Information security and risk is responsible for security administration, intrusion detection, security monitoring, and business-recovery planning.
   - Operational services performs day-to-day operation of servers and related peripherals.
   - System software services installs and tests system software releases, monitors daily system performance, and resolves system software problems.
   - Technical delivery services maintains job scheduling and report distribution software, manages security administration, and maintains policies and procedures manuals for the PAS processing environment.
   - Voice and data communications maintains the communication environment, monitors the network, and provides assistance to users and plan sponsors in resolving communication problems and network planning.

Procedures

The pension administration services covered by this system description include
1. pension master file maintenance,
2. contributions,
3. withdrawals,
4. investment accounting, and
5. reporting to members.

These services are supported by XITD, which supports PAS 24 hours a day, 7 days a week. The key support services provided by XITD include
1. systems development and maintenance,
2. security administration and auditing,
3. intrusion detection and incident response,
4. data center operations and performance monitoring,
5. change controls, and
6. business recovery planning.

Data

PAS data consists of the following:
1. Master file data
2. Transaction data
3. Error and suspense logs
4. Output reports
5. Transmission records
6. System and security files

Transaction processing is initiated by the receipt of paper documents, electronic media, or calls to XYZ Co.'s call center. Transaction data is processed by PAS in either the online or batch mode and is used to update master files. Reports are available either in hard copy or through a report-viewing facility to authorized users based on their job functions. Pension statement and transaction notices are mailed to plan sponsors and members.

Period of Coverage

The service auditor and the service organization may decided to issue a point-in-time report or a report that covers a period. The following factors should be considered in deciding which type of report to issue.

- The anticipated users of the report and their needs.
- The need for contiguous coverage between reports.
- The degree and frequency of change in each of the system components.
- The cyclical nature of processing within the system.
- Historical information about the system.

CPA Canada and AICPA require that if a period is to be covered, it should not be fewer than six consecutive months.

Subsequent Events

Events or transactions sometimes occur subsequent to the point in time or period of time covered by the service auditor's report but prior to the date of the report, that have a material effect on the system or control criteria, or that require adjustment or disclosure in the report. In performing an attest engagement, an auditor should consider information about subsequent events that comes to his or her attention. Two types of subsequent events require consideration by the auditor.

The first type consists of events that provide additional information with respect to conditions that existed at the point in time or during the period of time covered by the service auditor's report. This information should be used by the auditor in considering whether the subject matter or assertion is presented in conformity with the criteria and whether it affects the presentation of the subject matter, the assertion, or the service auditor's report. An example of this type of event is that a disaster recovery test carried out subsequent to the report period failed because data backup in the report period was done incorrectly. The auditor should assess the significance of this control failure and consider qualifying the report. If the control failure is not significant, there is no need to disclose this subsequent event in the audit report.

The second type consists of those events that provide information with respect to conditions that arose subsequent to the point in time or period of time covered by the practitioner's report that are of such a nature and significance that their disclosure is

necessary to keep the subject matter from being misleading. This type of information will not normally affect the audit report if the information is appropriately disclosed by the service organization. An example is the collapse of the data center.

Although the service auditor has no responsibility to detect subsequent events, s/he should inquire of the service organization as to whether they are aware of any subsequent events, through the date of the audit report, that would have a material effect on the subject matter or assertion. The representation letter ordinarily would include a representation concerning subsequent events. The service auditor has no responsibility to keep informed of events subsequent to the date of his or her report; however, s/he may later become aware of conditions that existed at that date that might have affected the audit report had s/he been aware of them.

Illustrative SysTrust opinion

The following is an illustrative opinion provided by CPA Canada and AICPA.

To the management of ABC Company, Inc.:

We have examined management's assertion that during the period [*month, day, and year*] through [*month, day, and year*], ABC Company, Inc. (ABC Company) maintained effective controls over the _____ [*type or name of system*] system based on the AICPA and CPA Canada trust services availability, security, processing integrity, and confidentiality criteria to provide reasonable assurance that

1. the system was available for operation and use, as committed or agreed;
2. the system was protected against unauthorized access (both physical and logical);
3. the system processing was complete, accurate, timely, and authorized; and
4. information designated as confidential was protected by the system as committed or agreed based on the AICPA and CPA Canada trust services security, availability, processing integrity, and confidentiality criteria.

ABC Company's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the _____ [*type or name of system*] system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the Chartered Professional Accountants Canada and, accordingly, included (1) obtaining an understanding of ABC Company's relevant controls over the availability, security, processing integrity, and confidentiality of the _____ [*type or name of system*] system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or

failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CPA Canada trust services security, availability, processing integrity, and confidentiality criteria.

[*Name of CPA firm*]
Chartered Professional Accountants

PAYMENT CARD INDUSTRY SECURITY STANDARD

The Payment Card Industry (PCI) Security Standard was introduced in 2004 by American Express, Diners Club, Discover Card, JCB International, MasterCard, and Visa to prevent credit card theft. These credit card issuers expect merchants, information technology (IT) service organizations and financial institutions to comply with the standard. The standard is maintained by the PCI Security Standard Council (PCISC) whose membership includes the six major credit card issuers.

The PCI Security Standard has the following twelve high level requirements. Each of these high level requirements is further explained in detailed requirements, which we will discuss later in this chapter.

1. Install and maintain firewall and router configurations to protect cardholder data.

2. Do not use vendor supplied defaults for system passwords and other security parameters.

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across public, open networks.

5. Use and regularly update anti-virus software on all systems commonly affected by malware.

6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data on a need-to-know basis, including encryption of any stored card number.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to cardholder data and network resources.

11. Regularly test security systems and processes.

12. Maintain a policy that addresses information security.

The above requirements apply to an organization's cardholder data environment, i.e., the IT environment and systems that process and store credit card transactions. Credit card issuers (e.g., Visa and MasterCard) require large merchants (including not-for-profit organizations and governments) to obtain annual external validation of compliance. For example, Visa has defined the following classes of merchants for compliance. Failure to comply may lead to penalty imposed by the card issuer.

Level	Definition	Compliance Requirement
1	Any merchant (regardless of acceptance channel) processing over 6,000,000 Visa transactions per year. Any merchant that Visa, in its sole discretion, determines should meet the Level 1 Merchant requirements, to minimize risk to the Visa system.	a. Annual On-Site PCI Data Security Assessment by a qualified security assessor (QSA) approved by PCISSC. Every other year, this on site review may be conducted by internal audit instead of a QSA provided there has been no change in infrastructure and the Acquirer agrees. b. Quarterly network security scan by a PCISSC Approved Scanning Vendor (ASV). c. Annual PCI Self Assessment Questionnaire submitted to the Acquirer. The results must be submitted to the Acquirer. An Acquirer is a financial institution that accepts credit card transactions from a merchant.
2	Any merchant (regardless of acceptance channel) processing 1,000,000 to 6,000,000 Visa transactions per year.	Requirements (b) and (c) above.
3	Any merchant processing 20,000 to 1,000,000 Visa eBusiness transactions per year.	Requirements (b) and (c) above.
4	Any merchant processing 1 - 20,000 Visa eBusiness transactions per year, and all other merchants (regardless of acceptance channel) processing 20,000 to 1,000,000 Visa transactions per year.	Requirement (c) above.

PCISC has provided the following guidelines on each of the twelve high level standards. I have added some explanatory notes to these guidelines.

Firewall Configuration

1. There must be a formal process for approving and testing firewall connections as well as changes to configuration of firewalls and routers.

2. There must be current network diagrams with connections to cardholder data, including wireless connections.

3. There must be a firewall at each Internet connection as well as between a demilitarized zone (DMZ) and an internal network.

4. Groups, roles and responsibilities for logical management of network components must be defined.

5. Document with business justification the use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to file transfer protocol, Telnet, POP3 (Internet email) and Internet Message Access Protocol (IMAP). IMAP is a common Web mail protocol that allows users to access email on a remote server.

6. Review firewall and router rules semi-annually.

7. Restrict external network access to the cardholder data environment (CDE). CDE is defined as an area of computer system network that processes cardholder data or sensitive authentication data and those systems and segments that are directly attached to or support cardholder processing, storage, or transmission.

8. Restrict inbound and outbound traffic to that which is necessary in CDE.

9. Secure and synchronize router configuration files.

10. Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.

11. Limit inbound traffic to IP addresses in the DMZ.

12. Implement stateful inspection firewalls.

13. Place system components that store cardholder data in an internal network zone, segregated from the DMZ and other untrusted networks.

14. Do not disclose private IP addresses and routing information to external parties.

15. Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

Vendor Supplied Defaults

1. For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

2. Develop configuration standards for all system components to comply with industry accepted system hardening standards.

3. Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.

4. Enable only necessary and secure services as well as protocols, etc., as required for the function of the system.

5. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

6. Protect and restrict all system administrative access not carried out at the server with strong cryptography. This means encrypting remote administration activities.

7. Shared hosting providers must protect each entity's hosted environment and cardholder data.

Protect Stored Cardholder Data

PCISC has placed the following restriction on cardholder and authentication data storage.

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

1. *Sensitive authentication data must not be stored after authorization.*
2. *Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.*

The service code is embedded in the chip or stripe and contains the following information.

First digit

1: International interchange OK
2: International interchange, use IC (chip) where feasible
5: National interchange only except under bilateral agreement
6: National interchange only except under bilateral agreement, use IC (chip) where feasible
7: No interchange except under bilateral agreement (closed loop)
9: Test

Second digit

0: Normal
2: Contact issuer via online means
4: Contact issuer via online means except under bilateral agreement

Third digit

0: No restrictions, PIN required
1: No restrictions
2: Goods and services only (no cash)
3: ATM only, PIN required
4: Cash only
5: Goods and services only (no cash), PIN required
6: No restrictions, use PIN where feasible
7: Goods and services only (no cash), use PIN where feasible

The CAV2/CVC2/CVV2/CID code is the 3 digit code on the back of the card to be requested for “card not seen” purchases. The PIN block is the encrypted PIN.

In addition, the following requirements have to be met.

1. Implement a data retention and disposal policy that includes:
   _ Limiting data storage amount and retention time to that which is required for legal, regulatory and business requirements.
   _ Processes for secure deletion of data when no longer needed.
   _ Specific retention requirements for cardholder data
   _ A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.

2. Do not store the card verification code or value (the 3-digit or 4-digit number on the back of the card) used to verify card-not-present transactions. This code is a hash of the card number and expiry date.

3. Do not store the personal identification number (PIN).

4. Do not display the entire credit card when confirming to a customer or the third party. The maximum digits to be displayed are the first 6 and the last 4.

5. Do not store credit card numbers in easily recognizable plain text. PCI recommends strong encryption.

6. Document the encryption key management process.

Develop and Maintain Secure Systems and Applications

1. Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

2. Separate development, test and production environments with appropriate segregation of duties.

3. Do not use production data for testing or development.

4. Test security patches.

5. Have fall-back procedures.

6. Develop systems to prevent structured query language injection and buffer overflow.

Assign a Unique ID to Each Person with Computer Access

1. Incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties.

2. Set passwords for first-time use and reset to a unique value for each user, requiring a change immediately after the first use.

3. Immediately revoke access of any terminated users.

4. Remove or disable user IDs after 90 days of inactivity.

5. Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access.

6. Do not use group, shared, or generic accounts and passwords.

7. Change passwords at least every 90 days.

8. Require a minimum password length of 7 alphanumeric characters.

9. Do not allow reuse of the last 4 generations of passwords.

10. Lock out users after 6 unsuccessful password attempts for 30 minutes or until reactivated by the system administrator.

11. Lock the screen after 15 minutes of inactivity.

12. Control addition, change and deletion of user profiles.

Restrict Physical Access to Cardholder Data

1. Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

2. Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.

3. Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

4. Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.

5. Make sure visitors are:
   - authorized before entering an area where cardholder data is processed or maintained;
   - given a physical token that expires and identifies the visitor as such;
   - asked to surrender the token when leaving the area.

6. Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.

7. Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.

8. Physically secure all media

9. Classify media based on information sensitivity.

10. Send the media by secured courier or other delivery method that can be accurately tracked.

11. Properly maintain inventory logs of all media and conduct media inventory counts annually.

12. Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

13. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

Track and Monitor All Access to Cardholder Data and Network Resources

These guidelines apply to merchants and eBusiness service organizations which are required to provide annual validation of PCI Security Standard compliance. They also apply to financial institutions.

1. Establish a process for linking all access to system components to individual users.

2. Secure audit trails so they cannot be altered.

3. Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection systems, firewalls, intrusion prevention systems, authentication and authorization.

4. Retain audit trail history for at least one year.

Regularly Test Security Systems and Processes

These guidelines apply to merchants and eBusiness service organizations which are required to provide annual validation of PCI Security Standard compliance. They also apply to financial institutions.

1. Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

2. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. The external scans must be done by a PCI approved scanning vendor.

3. Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. These penetration tests must include the network and application levels.

4. Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

5. Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparison weekly.

Maintain a Policy That Addresses Information Security

These guidelines apply to merchants and eBusiness service organizations which are required to provide annual validation of PCI Security Standard compliance. They also apply to financial institutions.

1. Include an annual process that identifies threats, vulnerabilities and results in a formal risk assessment.

2. Review the security policy annually.

3. Develop daily operational security procedures.

4. Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, smart phones, e-mail usage and Internet usage) and define proper use of these technologies.

5. Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

6. Assign to an individual or team the following information security management responsibilities:
    - Establish, document, and distribute security policies and procedures.
    - Monitor and analyze security alerts and information, and distribute to appropriate personnel.
    - Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situation.
    - Administer user accounts, including additions, deletions, and modifications.
    - Monitor and control all access to data.

7. Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
    - Education personnel upon hiring and annually.
    - Require personnel to acknowledge at least annually that they have read and understood the security policy.

8. Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.

9. If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:
    - Maintain a list of service providers.
    - Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider possesses.
    - Ensure there is an established process for engaging service providers including proper due diligence prior to the engagement.
    - Maintain a program to monitor service providers' PCI DSS compliance status annually.

10. Create an incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:
    - Roles and responsibilities as well as communication and contact strategies to be deployed in the event of a compromise including notification of the payment brands.
    - Specific incident response procedures.
    - Business recovery and continuity procedures.
    - Data back-up processes.
    - Analysis of legal requirements for reporting compromises.
    - Coverage and responses of all critical system components.
    - Reference or inclusion of incident response procedures in the payment brands.
    - Test the plan annually.
    - Designate specific personnel to be available on a 24/7 basis to respond to alerts.
    - Provide appropriate training to staff with security breach response responsibilities.
    - Include alerts from intrusion detection, intrusion-prevention, and file integrity monitoring systems.
    - Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

MANAGEMENT CHECKLIST

This checklist is intended for the management of an organization that hosts a system to be used by other organizations and also an organization that processes a large volume of credit card transactions.

1. Document the system descriptions and internal controls of systems used by other organizations.

2. Develop a process to monitor for system effectiveness regularly in order to assure user organizations.

3. If a SysTrust audit is pursued, assign ownership to an executive.

4. If a SysTrust audit is pursued, consider the applicability of the principles.

5. If a SysTrust audit is pursued, assess the applicability of control criteria and document control procedures for each criterion.

6. Assess the organization’s need to comply with the PCI Security Standard.

7. If the PCI Security Standard is applicable, set up a project to achieve compliance.

8. If the PCI Security Standard is applicable, assign an executive to be accountable for compliance.

9. Include PCI compliance in the organization's risk register and risk reports to the board of directors.

10. Select the PCI Qualified Security Assessor and Approved Scanning Vendor in accordance with the organization's procurement policy.

CONCLUSION

Technology trends like cloud computing, edge computing and software as a service increase the need for system operators to provide assurance to system users about information reliability. SysTrust is a comprehensive framework used to provide assurance to user organization management.

The Payment Card Industry Security Standard is also gaining prominence as more merchants, financial institutions and eBusiness service providers realize that they need to be serious about preventing credit card fraud. In the process of complying with the PCI standard, many organizations have come to realize that their networks and security infrastructures have significant holes. The success of the PCI framework can be measured by comparing credit fraud statistics over time as more organizations come to comply with this standard.

SUMMARY OF MAIN POINTS

1. A SysTrust audit is intended to provide assurance to user organizations of a system hosted external to the organizations that the system is reliable from the perspective of security, processing integrity, availability, confidentiality and privacy protection.

2. A firm must be licensed by CPA Canada or AICPA specifically for SysTrust in order to perform a SysTrust audit.

3. A SysTrust audit can provide point-in-time assurance or assurance over a period.

4. PCI Security Standard applies to all merchants, IT service organizations and financial institutions that process credit card transactions electronically.

5. Large merchants and large organizations that accept credit card payments for goods, services or donation for payments are procure at least annual independent validation of compliance.

6. All organizations that accept credit card payments for goods, services or donations must provide an annual self assessment compliance checklist to their financial institutions

7. The PCI Security Standard applies only to the Cardholder Data Environment, a network environment where a substantial quantity of cardholder data is stored or processed.

REVIEW QUESTIONS

1. Map the SysTrust principles to the control matrix in Chapter Six.

2. What are the management options to avoid a qualified SysTrust audit opinion when a significant control deficiency is found?

3. What does the SysTrust audit opinion cover?

4. What parties can benefit from a SysTrust report?

5. What kinds of organizations are held to comply with the Payment Card Industry Security Standard?

6. What kinds of organizations are required to provide an annual external validation of compliance with the PCI Security Standard?

7. According to the PCI Security Standard, what kinds of access should be monitored?

8. How does the PCI Security Standard affect the profit of large retail merchants?

CASE #1 – Independent Electricity System Operator

The Independent Electricity System Operator (IESO) works at the heart of Ontario's power system, connecting all participants – generators that produce electricity, transmitters that send it across the province, retailers that buy and sell it, industries and businesses that use it in large quantities and local distribution companies that deliver it to people's homes. Every five minutes, the IESO forecasts consumption throughout the province and collects the best offers from generators to provide the required amount of electricity. This allows hydro companies and their industrial customers to see price fluctuation based on supply and demand. As a result, they can shift consumption away from peaks in demand to times when the price is lower.

The IESO monitors the system and identifies what is required to maintain reliability in the future, reporting on these recommendations through regular publications. In its quarterly 18-month forecasts of the growth in demand for electricity, the IESO assesses whether there will be adequate generation and transmission facilities. In addition, the IESO prepares the semi-annual Ontario Reliability Outlook, which reports on the progress of interrelated generation, transmission and demand-side projects underway to meet Ontario's reliability requirements.

The IESO continues to work with other stakeholders to evolve the market for the benefit of all. Further enhancements will strengthen the market, enhance reliability and provide Ontarians with greater access to information about their power system.

IESO is a not-for-profit corporate entity established in 1998 by the Electricity Act of Ontario. It is governed by an independent Board whose members are appointed by the Government of Ontario. Its fees and licences to operate are set by the Ontario Energy Board and it operates independently of all other participants in the electricity market.

The IESO has full statute-based authority for establishing, monitoring and enforcing reliability standards in the province. All the companies that make up the power system in Ontario must meet the IESO's standards.

Source: http://www.ieso.com/imoweb/siteShared/whoweare.asp?sid=bi, *accessed on May 2, 2014.*

Required

Describe how the SysTrust model can be applied to IESO.

CASE #2 – PCI Data Security Assessment

A merchant that processes more than $6 million Visa transactions is required to conduct an annual data security assessment. Assume you are a Qualified Security Assessor, prepare an audit program to address 1 of the 12 high level standards.

RUNNING CASE – Blackberry

Does SysTrust apply? Is Blackberry held to comply with the PCI Security Standard? Does Blackberry add any value to PCI compliance?

MULTIPLE CHOICE QUESTIONS

1. Which of the following pair of SysTrust principles are most similar?
   A. Confidentiality and privacy
   B. Security and processing integrity
   C. Processing integrity and availability
   D. Availability and privacy

2. Who is the primary audience of a SysTrust report?
   A. Service organization management
   B. Shareholders' auditors of service organization
   C. User organization management
   D. Shareholders' auditors of user organizations

3. Who is responsible for developing control procedures in a SysTrust engagement?
   A. External auditors
   B. Service organization management
   C. Internal auditors
   D. User organization management

4. Which SysTrust principle addresses application controls the most?
   A. Security
   B. Confidentiality
   C. Processing integrity
   D. Availability

5. Which organization is most likely exempted from obtain external scanning for compliance with the PCI Security Standard?
   A. Sony
   B. Amazon
   C. Boeing
   D. Walmart

6. What kind of access to cardholder data must be monitored by Best Buy?
   A. All
   B. Update
   C. External
   D. Create

7. Who make up the PCI Security Council?
   A. Large banks
   B. Major credit card issuers
   C. Large online merchants
   D. Federal Reserve Board

8. What is the maximum number of digits in a credit card number that can be displayed to a customer or a merchant?
   A. First 6 and last 4
   B. First 6
   C. Last 4
   D. First 10
   E. First 4 and last 4

Chapter 11 – COMPUTER CRIME

Technological progress is like an axe in the hands of a pathological criminal. –

*A*lbert Einstein

Computer crime has increased in volume, impact and variety in the last twenty years mainly because of the Internet. There are broadly speaking, two types of computer crime: crime causing fairly immediate damage like hacking, and crime that is fraudulent like an email scam. In either case, the crime may be committed on IT resources or it may use IT as a tool to achieve the criminal intent.

Here is a list of recently publicized computer crimes.

- On May 19, 2014, law enforcement agencies in 16 countries, including Canada, arrested 97 people accused of developing, distributing or using the Blackshades malware. This malware allows one to control a remote computer including turning on the webcam. This technology is used by law enforcement agencies and computer support people for troubleshooting. A criminal can copy files and use them to hold the victim to ransom.
- In April 2014, less than a week after Royal Canadian Mounted Police was notified of a malicious cyber attack that resulted in the theft of 900 social insurance numbers from the Canada Revenue Agency's website, a 19-year-old London, Ontario man became the first person to be arrested in connection with the Heartbleed security bug.
- In November 2013, the UK National Crime Agency's National Cyber Crime Unit (NCCU) warned of a mass email-borne malware campaign aimed at small and medium enterprises (SMEs) and consumers. The emails appeared to be from financial institutions, but carry malicious attachment that can install Cryptolocker malware, a type of ransomware. The NCA warning came a week after the US computer emergency response team (US-Cert) issued a similar warning to US computer users. Security firm BitDefender found that in the week starting 27 October 2013, more than 12,000 computers in the US were infected with the Cryptolocker malware. The malware was designed to encrypt files on the infected computer and any network it was attached to and then demand the payment of a ransom of around £500 in Bitcoins to unlock the files.
- Sonya Martin, 45, of Chicago, a lead member in one of the most sophisticated and organized computer hacking and ATM cashout schemes ever perpetrated, was sentenced on August 21, 2012 by United States District Judge Steve C. Jones to serve two years and six months in federal prison on charges of conspiracy to commit wire fraud. During November 2008, an elite group of hackers obtained unauthorized access into the computer network of WorldPay US, Inc., then-known as RBS WorldPay, a payment processor located in Atlanta. The hackers

used sophisticated techniques to compromise the data encryption that was used by WorldPay to protect customer data on payroll debit cards. Payroll debit cards are used by various companies to pay their employees. By using a payroll debit card, employees are able to make purchases or withdraw their salaries from an ATM. Once they compromised the encryption, the hackers raised the balances and ATM withdrawal limits on compromised accounts, and provided a network of lead "cashers" with 44 debit card account numbers and their associated PINs, which were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. The $9 million loss occurred within a span of less than 12 hours on November 8, 2008. Throughout the cashout, the hackers monitored the fraudulent ATM withdrawals in real-time from within the computer systems of WorldPay. Once the withdrawals were completed, the hackers sought to destroy data stored on the card processing network in order to conceal their illegal activity. WorldPay nevertheless discovered the unauthorized activity and immediately reported the breach. Sonya Martin worked with one of the lead cashers and supervised a cashing crew in Chicago. Martin was given a payroll card number and PIN code, and manufactured counterfeit debit cards based on that information. She gave the counterfeit cards to underlings she recruited and supervised, and together they fraudulently withdrew approximately $80,000 from various Chicago ATMs during the early morning hours of November 8, 2008. Martin, whose primary residence is in Nigeria, was arrested in March 2011 outside JFK airport in New York on her way to London.

- In June 2011, Spanish police reported that it had arrested three members of a local Anonymous group in three separate cities, claiming they were responsible for the hacking attacks against the PlayStation Store. Anonymous is a group initiating active civil disobedience and spread through the Internet while staying hidden. The police alleged that these three individuals were leaders of the group, and considered them to be some of the masterminds behind the attack. In addition to being charged with the PlayStation store hacks, these three were accused of leading hacks against government websites of a number of countries, two Spanish banks, an Italian energy company, and the website of the Spanish Electoral Board.

- One of the biggest frauds in financial services history was carried out by a 31-year-old trader in Société Générale's Paris headquarters, Jerome Kerviel. The trader took massive fraudulent directional positions – bets on future movements of European stock indices, without his supervisor's knowledge, the Bank said. Because he had previously worked in the trading unit's back office, he had in-depth knowledge of the control procedures and evaded them by creating fictitious transactions to conceal his activity. The back office checks trades to ensure that they are not correctly recorded. It also carries processes the required money transfers. The fraud was discovered on January 20, 2008. Société Générale (SocGen), one of the largest banks in Europe, started to unwind the positions the next day just as global equity markets were tanking on fears of a U.S. recession. "It was the worst possible time," says Janine Dow, senior director for financial

institutions at the Fitch ratings agency in Paris. SocGen, which also announced a nearly $3 billion 2007 loss related to U.S. mortgage-market woes, had to seek a $5.5 billion capital increase.

Here are the common types of computer crime that are not quite fraudulent in nature and that cause immediate damage.

- Altering a public computer system like a bank system without approval – Main control is a firewall.
- Deliberately spreading viruses and worms – Main controls include anti-virus software and patching.
- Email interception – Main control is encryption.
- Hacking – Main control is a firewall.
- Sabotage of computer equipment – Main control is physical security.
- Spreading, uploading or storing child pornography – Main control is web filtering.
- Theft of computer equipment – Main control is physical security.
- Theft of information – Main control is encryption.
- Theft of software – Main controls include access control list, digital rights control and management monitoring.

The following is a list of common computer frauds.

- ATM skimming – Main controls include user education and a surveillance camera.
- Changing computer system information to hide defalcation – Main controls include a firewall and access control lists.
- Computer scam – Main control is user education.
- Gaining unauthorized access to systems to transfer funds – Main control is an access control list.
- Identity theft – Main controls include user education and access control lists.
- Producing fictitious transactions – Main controls include segregation of duties and management review.

These lists are just common examples of information technology (IT) crime. These lists are just common examples of information technology (IT) crime. A lot of other crimes can be committed with the aid of computers, e.g., lapping, by diverting cash receipts and using later payments from other customers to post to the customer accounts whose

payments have been pocketed by the fraudulent employee, i.e., playing a "Ponzi" like delay trick. In this trick, a cash receipts clerk who knows the system well can use it to time the misappropriation of payments. This chapter is not intended to discuss all business crimes and accounting frauds. It focuses on IT crimes and frauds. However, for non-IT crimes, many system controls can be used to prevent or detect them. These controls are discussed in Chapters 3, 6 and 8.

Computer crime is committed because of temptation and opportunity. An opportunity to a criminal is created when internal controls are weak. Temptation is present when vulnerable assets are easily accessible.

INTERNAL CONTROLS

Here are the common internal controls against computer crime.

- Access control list
- Access log
- Cash receipts analysis to detect lapping - Analyzing the amounts and dates of cash receipts in relation to the outstanding balances and due dates at the time of posting, taking into consideration new purchases that would not yet be due for payment, generally 30 days from invoice dates. This will serve to detect lapping as the fraudster may not find customers that have the exact balances of the customers whose payments have been diverted and also the customers whose payments have been misappropriated would usually be shown by the accounts receivable system to have missed the due dates by a day or two because of lapping.
- Chief ethics officer
- Code of business conduct
- Digital certificate
- Digital rights monitoring
- Digital signature
- Encryption
- Exception reporting
- File blocking
- File integrity monitoring
- Firewall

- Intrusion detection system
- Intrusion prevention system
- Locks
- Management and independent review
- Password policy
- Password system configuration to comply with the password policy
- Security check for sensitive positions including criminal record check
- Security education
- Segregation of duties
- Web filtering
- Web site refresh
- Whistle blowing policy

Many of these controls are covered in Chapter Eight and Chapter Nine. We will describe the others below.

Chief Ethics Officer

Large organizations increasingly have an executive titled chief ethics officer. This is part of setting the tone at the top. This new position was created by many organizations to deter fraud by raising the awareness of ethics. Some organizations also include a compliance function in this position. Governments are also increasingly instituting such a function.

It must be clear to management that the chief executive officer (CEO) has ultimate responsibility for ethics. The chief ethics officer's job is to create a work environment where people frequently think about ethics, have good understanding of what is ethically acceptable and feel comfortable about coming forward and raising concerns. The chief ethics officer owns and administers the whistle blowing policy that tells people under what conditions they can go to the chief ethics officer to report suspected improper acts and that there will be no reprisal as a consequence.

Code of Business Conduct

One of the first tasks of a chief ethics officer is to document a code of business conduct and establish a process for communication to everyone in the organization and regular reminder about the code. The code tells employees and consultants what not to do when engaging in organization business or using organization resources. It addresses the following common topics:

- Unacceptable use of organization resources like viewing inappropriate sites or running a side business.
- Conflict of interest with suppliers, superiors, colleagues and subordinates.
- Avoiding fraud or potentially criminal activities.
- Reporting improper conduct, fraud or crime to the chief ethics officer following prescribed procedures.
- Respecting license restriction of software provided by the organization.
- Avoid using personal software on organization computers.
- Avoid using organization resources for personal purposes in a significant way.
- Acknowledging that employee activities in the organization or while conducting organization business are subject to monitoring by the organization.
- Respecting the confidentiality of organization information.

The code of business conduct should be supplemented with a policy on acceptable use of IT resources. This policy should state the types of unacceptable use of IT resources. Here is a common list of what is considered unacceptable.

- The use of corporate IT resources for excessive personal use.
- Using personal IT resources to conduct corporate business, unless approved by a manager.
- Accessing, displaying, downloading, creating, distributing or storing any software, graphics, images, text, music, video or other data which are offensive and conducive to a poisoned work environment, e.g., pornography.
- Using Internet sites for sharing files such as music files, video clips, digital image files or software programs, unless for corporate business.
- Streaming audio or video from the Internet, unless for corporate business purposes.
- Using corporate resources to play games.
- Operating a private business or political activities.
- Misrepresenting the organization's views on a matter.
- Discrediting others in the organization through electronic communications.
- Sending anonymous messages or impersonating others.
- Sending chain letters.
- Using offensive, threatening, abusive language in electronic communications.
- Using IT resources to discriminate against or harass, threaten or intimidate other employees or to create a hostile or humiliating work environment.
- Performing unauthorized network scans on, or conducting unauthorized access attempts to corporate systems, applications or services, or spreading viruses or malicious codes to other systems.

Employees should be educated about this policy upon joining the organization and reminded periodically. For example, a login script can be implemented to pop up a reminder that requires acknowledgement periodically when an employee logs on to the network. This policy should be enforced with system controls such as using a web filtering software system to deny web sites that fall into the above categories and track the types and extent of Internet use. Frequent Internet users should be flagged for reporting to managers who can then assess appropriateness in relation to job requirements.

Exception Reporting

Exception analysis can range from fairly simple tracking of account status like customers whose accounts get very close to the credit limits, to complicated multi-variable regression analysis and simulation to find insider trades or tax frauds. Large organizations like banks, securities regulators, insurance companies and governments use statistical analysis including data mining tools to detect insider trades, tax frauds, insurance frauds, defalcation and loan frauds. For example, Benford analysis is used by income tax departments to help in selecting questionable tax returns for audit. Statistical Analysis Software (SAS) is used by many large organizations to help them in customer relationship management systems and fraud detection. The following is a quote from the SAS web site, http://www.sas.com/solutions/fraud/index.html, accessed on May 7, 2014.

> *Banks, insurance companies, health care organizations and government entities are all seeing an increase in the incidence and sophistication of fraud, waste and abuse activities, fuelled in large measure by the financial turmoil gripping the world's economy. To fight fraud effectively, organizations must continually improve the monitoring of transactions across multiple accounts and systems. SAS® Enterprise Financial Crimes Framework provides a technology infrastructure that integrates fraud detection, alert management, network analysis and case management – giving organizations the upper hand in detecting fraud in any form, at any touch point.*

Statistical analysis is a powerful tool in that when numbers deviate from the norm, they require attention. For example, if the material cost of an aircraft deviates significantly from historical cost, it doesn't take an aeronautic engineer to suspect that something may be wrong.

When the population is large enough to form a base for comparison, even simple analytical review can lead to discovery of significant fraud. For example, a bank can calculate the following ratios every month for each branch and then compare the ratios for each branch to the overall ratios for the bank:

Interest revenue / non-interest revenue

Interest revenue / interest expense

Non-interest revenue / non-interest expense

Interest revenue / loan total

Interest expense / deposit total

Non-interest revenue / transaction volume

To be more granular, each branch's ratios can be compared to the ratios of the region or city; or each branch's ratios can be compared to the ratios for the types of branches, e.g., main branches, large commercial branches, urban branches, suburban branches and rural branches. The ratios should also be compared from period to period. There can also be correlation between ratios as the ratios between ratios should also be fairly stable. For example, if the interest revenue / non-interest revenue remains fairly stable but interest revenue / interest expense has decreased, there may be some significantly non-performing or fictitious loans. A fraudster may think that the difference between 2.3 and 2.4 is insignificant; however, if the historical difference in the last year has ranged from 2.28 to 2.32, 2.4 would be a significant deviation. Software tools can be used to query even much longer periods and much larger populations.

EVIDENCE

Evidence is crucial in any forensic investigation. Without credible evidence, prosecution, pursuit of compensation and disciplinary action will not be successful. There are four types of evidence in IT forensic.

1. Physical evidence includes tangible objects that can be physically carried into a court. Examples include a hard disk accompanied by a printout of its content and a phone log. Physical evidence speaks for itself.

2. Documentary evidence includes recorded information such as audio or video recording. Documentary evidence requires the collaboration of an expert witness.

3. Testimonial evidence includes testimony made under oath by witnesses as well as confessions and hearsay evidence. Examples include a security expert's opinion and a computer technician's statement of what s/he read or saw when fixing a computer.

4. Demonstrative evidence includes charts, graphs and computer reconstruction of data that expert witnesses or lawyers can use in testimonies or cross examinations.

When handling evidence, a forensic auditor must ensure the following:

- Evidence is not altered, damaged, contaminated or destroyed in the investigation procedures. Simply viewing data using a word processor can destroy important audit trail. This is why the entire hard disk should be imaged to an offline medium and data should be analyzed from the a copy of the image.

- No malicious software is permitted to infect or corrupt the subject computer, the auditor's computer or other computers on the subject's computer's network.

- All possible relevant evidence extracted from the subject's computer or network is fully preserved.
- An unbroken chain of custody is established, documented and maintained.
- The privacy and confidentiality of all data on the subject's computer and networks are properly maintained.

FORENSIC SOFTWARE

A popular forensic investigation software tool is Encase. It is used by police and large organizations like banks, large companies and governments. Here are the common functions.

- On site or remote imaging of a disk and RAM with MD5 or SHA-2 hash to preserve integrity. The hash is performed before imaging, after imaging and periodically to ensure that the entire disk has been imaged and the image has not been changed.
- File analysis to look for evidence.
- Data recovery from deleted files.
- Investigation case documentation organization.
- Investigation work papers and report templates.

Encase applies the Locard exchange principle, which says that every contact leaves a trace.

Investigations should also use other more focused tools for functions like searching email and archive files. Discovery Accelerator is one such tool. It is important that these tools be run from highly secured computers like offline computers in order to prevent tampering with the evidence. Emails can be downloaded and then analyzed using Discovery Accelerator.

FORENSIC INVESTIGATION PROCEDURES

The following are some common computer forensic investigation procedures to be carried out by internal forensic investigations within an enterprise. This checklist is not intended to be sufficient for police use.

1. Assess the situation and understand what type of incident or crime is to be investigated.

2. Obtain senior management approval to proceed with an investigation. The level of management should be several levels above the target individuals being investigated to avoid conflict of interest or abuse of the investigation process. For example, if the chief financial officer (CFO) wants the controller investigated, the organization's policy should require that the CFO's supervisor approves this before investigation begins.
3. Determine the equipment and software needed to carry out the investigation.
4. Apply packet sniffing.
5. Review system logs.
6. Seize evidence in real time, e.g., printing the screen, recording information on the screen, and taking pictures of what is on the screen.
7. Apply special software like Encase to image hard disks remotely or on site.
8. Apply special software like Encase to recover deleted data.

9. Avoid shutting down the suspected computers, connect uninterrupted power supply (UPS) to keep the computer on, so as to prevent loss of data or system audit trail. If UPS is not available and the computer has to be moved, unplug it instead of using the operating system to shut it down; unplugging will involve less interference with the audit trail.
10. Scan imaged drives and copied emails for viruses.
11. Back up the evidence.
12. Use the organization's PKI key recovery process to decrypt files. If that does not work, use password cracking software to obtain the password for the encryption key.

13. Boot the captured or suspected computers with an external boot disk instead of using the computer's operating system to avoid loss of audit trail.

14. Document all sequence of events, all interviews, time spent by each investigator and the work performed by each investigator.

15. Maintain arm's length with the people being investigated, the requester of the investigation, the approver of the investigation and people who provide information to investigators, to avoid conflict of interest.

16. Continuously assess the need to communicate with the legal department, senior management and the police.

17. Do not communicate information about the investigation using post mail or an unencrypted electronic medium.

18. Be a patient listener, ask open questions, make others comfortable in talking to you, take copious notes.

19. Safeguard the investigation files with encryption and physical measures.

20. Keep all evidence, including electronic media for a case all together as complete audit trail, with proper cross references to source, date, sequence of events etc.

21. Dispose of unneeded electronic evidence by using the organization's approved data wiping software and standard procedures, including if necessary, corporate approved vendors for media storage, backup and destruction.

MANAGEMENT CHECKLIST

1. Appoint a chief ethics officer.
2. Establish a code of business conduct including a whistle blowing policy.
3. Establish a policy on acceptable use of IT resources.
4. Obtain employee acknowledgement of understanding of the code of business conduct and the policy on acceptable use of IT resources regularly.
5. Establish a policy on reference check for new hires.
6. Establish a policy for conducting security check including criminal record check for positions that handle sensitive information or vulnerable assets.
7. Large organizations should establish a forensic investigation function.
8. Ensure the audit committee is made aware of all computer crime committed against the organization.
9. Ensure that the applicable labor unions are consulted with respect to the development and changes of the code of business conduct.
10. Establish a protocol for informing the police of criminal activities in or against the organization, involving the security and legal departments. The protocol should include procedures for providing audit trail, evidence and information to the police with respect to management approval, warrants and court orders; e.g., what documents and information can be provided to the police without a warrant or court order.

FORENSIC INVESTIGATION CHECKLIST

When computer crime is highly suspected or is known to have occurred, depending on the crime's scale and impact, management may want to order a forensic investigation. The objective of such an investigation includes:

- Confirming that crime has been committed within or on the organization.
- Collecting evidence and linking it to suspects.
- Collecting evidence to provide to the police or to support a civil litigation.
- Determining the people who committed or assisted in committing the crime.
- Root cause analysis with recommendations to improve internal controls.

A typical IT forensic assignment includes the following activities.

1. Determine the suspects, suspected computers and storage media.
2. Capture information from the suspected computers and storage media without leaving a trace on the computers and media, more importantly, without distorting the audit trail in the computers and media. This will require forensic tools like Encase. A common technique is to image the hard disk to preserve all audit trail. Simply copying files can distort the file access pointers and open up room for defence counsels to challenge the evidence.
3. Make a backup copy of the captured information and store it away. Perform analysis on another copy.
4. Scan for viruses.
5. Decrypt data files.
6. Determine the content of computer files.
7. Compare the content of computer files to known reference files or documents.
8. Determine the time and sequence in which the files were created or changed.
9. Recover deleted files.
10. Look for key phrases or key words.
11. Study and analyze emails, data files and source code.
12. Link evidence, analyses, interview notes and assessments in a case work paper file.
13. Encrypt analyses and evidence other than source data.
14. Physically protect the work paper file.
15. Logically protect the work paper file without tampering with source data or distorting the audit trail of source data.
16. Keep a copy of the work paper file and captured data offsite.

17. Determine the internal control weaknesses that let the fraud or crime occur.
18. Make recommendations to tighten internal control weaknesses.
19. Provide a report to senior management.
20. Provide information to law enforcement agencies with appropriate review by the organization's lawyers.

CONCLUSION

As the world is becoming more computer literate and organizations increasingly rely on computers, cyber crimes and computer related frauds are taking up a larger and larger portion of overall crimes. It doesn't take long for criminals to realize that a few clicks can land them much more money than holding up a bank. Identity theft is also growing, which can serve as the portal to other crimes like stealing real estate, obtaining business secret, money laundering and transferring money from the victim's bank accounts, filing tax returns in the names of the victims to obtain tax refunds, etc.

SUMMARY OF MAIN POINTS

1. Opportunity has to be present for computer crime to occur. Opportunity is created by internal control deficiency.

2. Two types of computer crime: crime that is not mainly deceitful like hacking, and computer fraud. Shareholders' auditors are more concerned about computer fraud as it carries more uncertainty.

3. IT resources may be the target of computer crime. IT resource may be used to commit a crime.

4. Preventing computer crime starts with appointing a chief ethics officer as well as educating employees and customers on what behavior and activities are unacceptable.

5. The CEO is ultimately accountable for ethics. The chief ethics officer is a facilitator.

6. ID theft is a common computer crime that can lead to other crimes.

7. Every large organization should establish a computer forensic investigation function to perform forensic investigations based on management requests, suspicions from control deficiencies and proactive scanning of employee IT network activities for anomalies

8. IT forensic assignments should involve obviously IT specialist and investigators with business and financial experience, the legal department, labor union representatives and the police (for computer crime).

REVIEW QUESTIONS

1. What are common computer crimes committed against financial institutions and retailers?

2. Who do you think the chief ethics officer should report to and why?

3. What computer crimes can result from identity theft?

4. What internal controls can organizations implement to prevent system alteration?

5. What are some system controls that can prevent or detect disbursement fraud?

6. What technology do you think the police and securities commissions use to detect insider trading?

7. How can a bank use analytical review to detect fictitious loans?

8. What is the relationship of Encase and disk wiping software?

CASE #1 – **Deloitte & Touche LLP v. Carlson**, 2011 WL 2923865 (N.D. Ill. July 18, 2011), U. S. District Court, State of Illinois.

Source: *http://blog.Internetcases.com/2011/07/27/computer-fraud-and-abuse-act-case-against-hard-drive-destroying-director-goes-forward/**, accessed on May 7, 2014.*

Defendant had risen to the level of Director of a large consulting and professional services firm. After defendant left the firm to join a competitor, he returned his work-issued laptop with the old hard drive having been replaced by a new blank one. Defendant had destroyed the old hard drive because it had personal data on it such as tax returns and account information.

The firm sued, putting forth a number of claims, including violation of the Computer Fraud and Abuse Act (CFAA). Defendant moved to dismiss for failure to state a claim upon which relief can be granted. The court denied the motion. Defendant argued that the CFAA claim should fail because plaintiff had not adequately pled that the destruction of the hard drive was done "without authorization." The court rejected this argument.

The court looked to Int'l Airport Centers LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) for guidance on the question of whether defendant's alleged conduct was "without authorization." Int'l Airport Centers held that an employee acts without authorization as contemplated under the CFAA if s/he breaches a duty of loyalty to the employer prior to the alleged data destruction.

In this case, plaintiff alleged that defendant began soliciting another employee to leave before defendant left, and that defendant allegedly destroyed the data to cover his tracks. On these facts, the court found the "without authorization" element to be adequately pled.

Required

1. What else could Carlson have done to keep his personal information from Deloitte when the laptop was returned?

2. How do you think Carlson communicated with the other employee whom he was alleged to have solicited to leave Deloitte?

3. What are some steps you think Deloitte might have used to find evidence of Carlson's loyalty breach or improper system activities?

CASE #2 – Societe Generale

In January 2008, Jerome Kerviel, a trader in France's banking giant Societe Generale (SocGen), caused losses totaling US$7 billion by creating fictitious transactions to offset bad trades. Bank officials said Kerviel had closed the fake trades just before the risk monitoring program could have triggered alerts. He also hacked the Bank's servers to circumvent the trade monitoring system. He stole the passwords of colleagues. Up until 2008, he was considered a smart and diligent trader and refused his supervisor's suggestion for him to take vacations. Some alerts were indeed produced by the trade monitoring system but Kerviel was able to explain them away to his boss.

SocGen is one of the world's most respected financial institutions. It was founded in 1864. There are 130,000 employees and 22 million customers. The bank's reputation was tarnished in 2008 by a rogue trader, Jerome Kerviel, an employee of the bank, who caused a loss of 5 billion euros.

Kerviel started working in the risk management department in the bank and learned its security procedures and back office systems quite well. He was then promoted to the bank's Delta One trading desk for index futures. The involved buying European stock

indices and selling similar indices as hedges. This was meant to be of low risk and the profit was derived from the spreads over a large transaction volume. In order to make "large profit" for the bank, probably to impress his peers and bosses, Kerviel falsified the hedging indices information in his trades. During 2006 and 2007, he once accumulated trading positions amounting to US$73 billion.

Knowing the schedule of internal control checking of trader's positions, Kerviel erased his fictitious trades just before the check was performed and reinstated them right afterwards. The temporary imbalances did not trigger an alert. To beat the bank's access controls that support segregation of duties, he used other employees' IDs to accomplish his "hiding" and "erasure" acts. During his tenure at Delta One, he developed software management tools and at one point accounted for half of the trading desk's profit. He very seldom took vacation.

Apparently, Kerviel's supervisors trusted him too much and was misled by him that he had accumulated gains amounting to $2 billion (which were never realized). The bank also reportedly failed to follow up rigorously on 75 alerts about his trading activities. In some cases, he explained them away by saying he had made a data input mistake and then provided the correct information which was again falsified, including giving the name of a banker in another bank that Kerviel claimed was the counterparty providing the hedge. In 2005, however, he was reprimanded for exceeding his trading limit in his transactions with Allianz SE Securities, and was told that he would be fired for doing so again. Yet, he was allowed to continue trading. The $2 billion false book gain should have alarmed his supervisors because Delta One was intended to achieve small profits regularly. One reason for the oversight could have been that, in those years, SocGen relied on equity derivative trading to generate 80% of the bank's profit. An equity derivative is a calculated financial instrument whose value depends on the value of its associated equity, e.g., a stock option. It is much less tangible than a stock because there is no associated corporate ownership. One of the reasons for the bank's failure to stop Kerviel was that at one time, his supervisor had much less trading experience than Kerviel did. Another reason was that managers did not share alerts.

Once the fraud was discovered, SocGen decided to unload his positions. But the markets were weak in January 2008. The day of SocGen's dumping of these securities, stock markets in Germany, London and Paris fell as much as 7%. The German index continued to fall in that week. This apparently caused the U S Federal Reserve to cut interest rates. Securities Exchange Commission investigated SocGen about its dumping for potential breach of securities laws because the mass selling was done just before the bank announced the fraud. Some analysts estimated that the fraud alone caused a loss of about 2 billion euros and the distressed prices in the dumping led to another loss of 5 billion euros. To cover the loss, SocGen raised new capital through J. P. Morgan and Morgan Stanley in the amount of €5.5 billion.

These losses later looked less significant when the following banks announced their subprime losses:

Citigroup	$18.0 billion
USB	13.5 billion
Morgan Stanley	9.4 billion
Merrill Lynch	8.0 billion
HSBC	3.4 billion
Deustche Bank	3.2 billion
Bear Sterns	3.2 billion

On January 20, 2008, the bank's CEO offered to resign but the board did not accept the resignation, apparently fearing that it would lead to a liquidator to be appointed as the CEO. Three days later, SocGen was in control of the situation after dumping the related securities and arranging for capital increase. It then informed President Nicholas Sarkozy, the European Central Bank and the U S Federal Reserve Bank. The CEO said the bank was still profitable for 2007. He also announced further subprime mortgage related losses amounting to €2 billion. In April, he eventually resigned, largely because of increasing media and government pressure. He remained as chairman. SocGen's failure to stop the fraud earlier helped BNP Paribas, its main competitor, to gain many new accounts.

Bank officials claimed that throughout 2007, Kerviel had been trading profitably in anticipation of falling market prices. They also accused him of exceeding his authority to engage in unauthorized trades totaling as much as €49.9 billion, a figure far higher than the bank's total market capitalization. Bank officials claim that Kerviel tried to conceal the activity by creating fictitious losing trades so as to offset his early gains.

The bank claimed Kerviel "had taken massive fraudulent directional positions in 2007 and 2008 far beyond his limited authority" and that the trades involved European stock index futures. Though bank officials said Kerviel apparently worked alone, skeptics question how unauthorized trading of this magnitude could go unnoticed. Kerviel's unassuming background and position have heightened the skepticism that he worked alone. Some analysts suggested that unauthorized trading of this scale might have gone unnoticed initially due to the high volume in low-risk trades normally conducted by his department. The bank said that whenever the fake trades were questioned, Kerviel would describe it as a mistake then cancel the trade, after which he would replace that trade with another transaction using a different instrument to avoid detection. Kerviel's lawyers, Elisabeth Meyer and Christian Charrière-Bournazel, said that the bank's managers "brought the loss on themselves"; accused the bank's management of wanting to "raise a smokescreen to divert public attention from far more substantial losses in the last few months"; and said that Kerviel had made the bank a profit of US$2 billion as of 31 December 2007.

Managers for Société Générale have described some of the means Kerviel employed to avoid the bank's internal controls and escape detection. Its Executive Chairman Daniel Bouton describes the pattern as like "a mutating virus" in which hundreds of thousands of trades were hidden behind offsetting faked hedge trades. Officials said Kerviel was careful to close the trades in just two or three days, just before the trades' timed controls would trigger notice from the bank's internal control system, and Kerviel would then

shift those older positions to newly initiated trades. Some experts have expressed skepticism of the bank's account, saying that a pattern of closing out trades within the three day cycle alleged could not be accomplished given the immense sums involved.

Kerviel is not thought to have profited personally from the suspicious trades. Prosecutors said Kerviel had been cooperative with the investigation, and told them his actions were also practiced by other traders in the company. Kerviel admitted to exceeding his credit limits, but claimed he was working to increase bank profits. He told authorities that the bank was happy with his previous year's performance, and was expecting to be paid a €300,000 bonus on a €60 million declared profit (approximately 0.5%) which illustrates the definition of "fair pay" in the French investment banks. Family members speaking out said the bank is using Kerviel as a scapegoat to excuse its recent heavy losses.

On January 24, 2008, Société Générale filed a lawsuit against Kerviel for creating fraudulent documents, using forged documents and making attacks on an automated system. The next day, police raided the Paris headquarters of Société Générale and Kerviel's apartment to seize his computer files. On January 26, he was taken into police custody.

The investigation included scrutinizing his personal cell phone records, exploring possible links to other individuals working at rival banks and private investment firms who may be involved. The police were investigating whether he worked alone, and whether any investors outside of Société Générale may have been tipped off in advance. Police were interested whether others were involved either in the trades themselves or received notice of the bank's impending sell-off before the details of the scandal were publicly disclosed.

Kerviel was formally charged on 28 January 2008 with abuse of confidence and illegal access to computers. He was released from custody a short time after. The charges filed carry a maximum three-year prison term. On January 29, 2008, investigating judges Renaud van Ruymbeke and Françoise Desset rejected the prosecutor's bid to charge Kerviel with the more serious crime of "attempted fraud".

His trial began on June 8, 2010. On October 5, 2010, he was found guilty and sentenced to 5 years of prison, with 2 years suspended, full restitution of the $6.7 billion which was lost, and a permanent ban from working in financial services. Caroline Guillaumin, a spokeswoman for Société Générale, stated that the restitution was "symbolic", and that the bank had no expectation that the sum would be paid. Olivier Metzner, Kerviel's lawyer, described the sentence as "extraordinary" and said that Kerviel would appeal. Kerviel's sentence was suspended.

On October 24, 2012, a Paris appeals court upheld the October 2010 sentence to 3 years in prison with 2 more suspended, and ordered him to reimburse 4.9bn euros to Société Générale for its loss.

In March 2014, a French high court upheld Kerviel's prison sentence but ruled he would not have to repay €4.9bn.

Since Kerviel's release, he has been hired by Lemaire Consultants & Associates, an information systems and computer security consulting firm. While awaiting a ruling on his legal appeal and still protesting SocGen's stance in his case, Kerviel met with Pope Francis in Rome and undertook a pilgrimage from Rome to Paris against the "tyranny of the markets".

Required

How do you think Kerviel beat the controls, be detailed. How could SocGen have prevented this?

RUNNING CASE – Blackberry

What kinds of computer crime can be conducted on Blackberry users? What can Blackberry, individual users, corporate customers and wireless carriers for Blackberry prevent these crimes?

MULTIPLE CHOICE QUESTIONS

1. Which address is most useful in a forensic investigation?
    A. IP
    B. MAC
    C. URL
    D. Email

2. If a forensic auditor inspects a computer containing a critical file that is known to be highly encrypted but currently opened, what should the auditor do immediately?
    A. Pull the plug on the computer.
    B. Perform an orderly shutdown of the computer.
    C. Make an immediate shadow volume copy of the entire hard drive.
    D. Browse the open file.

3. Which medium should a forensic investigator target if a workstation's hard disk has been thoroughly wiped by a fraudster using Tabernus, a commercially accepted disk wiping software tool, say seven times?
    A. Firewall log
    B. Network drive
    C. Anti-virus log
    D. Sandbox

4. What computer crime does a firewall mitigate against?
    A. Hacking
    B. Identity theft
    C. Virus spreading
    D. ATM skimming

5. Which of the following techniques or tools is most useful to detect a bank loan fraud committed by a branch manager?
    A. Benford analysis
    B. Firewall
    C. Segregation of duties
    D. Discovery Accelerator

6. Which of the following crime is most commonly committed with ID theft?
    A. Hacking
    B. Virus spreading
    C. Loan fraud
    D. Child pornography

7. When of the following events must be reported to police?
    A. Employee found to be sending hate propaganda.
    B. A customer sent email to other customers to discredit the company.
    C. Many child pornography pictures found in an employee's shared network drive.
    D. A vendor has overbilled by $1 million and been paid.

8. When an investigator images an employee's hard disk and performs data analysis, what is the most relevant objective?
    A. Connecting suspect to evidence
    B. Connecting evidence to traces
    C. Obtaining testimony
    D. Determining network breach

9. If an investigator comes across an opened file that seems to contain criminally implicating information, what is the next step?
    A. Pull the plug.
    B. Study the file.
    C. Power down the computer.
    D. Image the hard disk.

10. What type of evidence is most readily prepared using Encase?
    A. Physical
    B. Demonstrative
    C. Testimonial
    D. Documentary

Glossary

Access control list	A list of users or programs that are authorized to access a specific resource like a file, indicating the type of access, e.g., read, write.
Access point	A wireless router connected to a wired network.
ACL	Audit Command Language, the most popular general audit software tool.
Action Center	A Windows facility for security configuration and repository of security settings.
Active Directory	Active Directory serves as a central location for network administration and security. It is used for authenticating and authorizing all users and computers within a network of Windows domain type, assigning and enforcing security policies for all computers in a network and installing or updating software on network computers.
Active X	ActiveX control is a framework for writing reusable code. Users should configure the browser to not accept unsigned ActiveX components automatically. ActiveX components usually are not run in the sandbox and therefore riskier than .NET components.
Advanced Encryption Standard	An advanced symmetric standard that uses symmetric algorithms that require 128-bit or 256-bit keys.
Architecture	The design and layout of a system's infrastructure.
ASCII	American Standard Code for Information Interchange is the personal computer data format; some people use it to refer to only alphanumeric data.
Asymmetric encryption	A pair of related keys are used. Something encrypted with one key can be decrypted with the other key.
Authenticode	Authenticode is Microsoft's tool for software distributors to digitally sign the software and for browsers to verify the digital signatures. It is a high risk for a user to select the enable option for running .NET Framework reliant components not signed with Authenticode.
Back door	A hole in software left open by accident or intent to allow an alternate method to access a system. A backdoor by design allows system administrators to perform quick fixes.

Batch system	A system that updates the master file(s) periodically by processing batches of transactions instead of each transaction in real time. A common example is payroll.
Batch total	A control total of an amount or quantity taken at one point of a transaction cycle for a batch system and agreed to another control total of the same batch of transactions taken at a later point to confirm completeness of processing.
Benford Law	A statistical distribution that indicates that the leading digits of a natural number are more likely to be a low order digit like 1 or 2 than being a high order digit like 9 or 8.
Big data	Big data means collecting large volumes of data beyond business transactions, that are somehow related to an organization's business in order to set more competitive strategies and make better informed corporate and business development decisions.
Boundary checking	Checking that the data input in a Web application does not exceed the field length expected by the application, to prevent buffer overflow.
Buffer overflow	A hacking technique to put in more data than requested in an Internet application to overflow the buffer of real access memory (RAM) allocated to the requested input and therefore overwrite some data in RAM allocated to other applications, causing havoc.
Business impact analysis	Analysis of disaster or business interruption scenarios and their impact on an organization's business. The purpose is to decide on the scope of a disaster recovery plan.
Certificate authority	An organization that issues digital certificates, usually for a fee.
Challenge response	Asking pre-arranged security questions of the user to help authenticate the access attempt.
Check digit	Using the last digit of a control number like a product number to validate data entry. The check digit is a derivative of the preceding digits. Social security and social insurance numbers (SIN) are also subject to this control. This control helps ensure valid, but not necessarily correct control numbers; e.g., if I give my wife's SIN to my employer, it would still pass the check digit test because it is a valid SIN.

CICS	Customer Information Control System (CICS) provides the software framework in IBM Z series severs for programmers to develop online real time systems that process customer transactions, like banking systems. It is not a programming language.
Click fraud	Clicking on a commercial link without the intent to learn about or buy the product or service. The intent here is mainly to cause a company to pay more for online advertising.
Cloud computing	Using distant servers in other networks to share computing and storage loads so as to reduce computing cost.
COBIT	Control Objectives for Business and Information Technology, published by Information Systems Audit and Control Association. It is a comprehensive of IT internal control objectives and generic procedures (automated and manual) widely adopted by large organizations.
Code comparison	A software change control that compares source code or object code between periods to detect changes in order for the changes to be reconciled to audit trail. Where an organization does not have source code, e.g., a purchased package, object code can be compared.
Cold site	An alternate disaster recovery site that is available in several days to a week. It takes time for the organization to arrange hardware and software to be moved into the site.
Compliance scanning	Use security software to scan system configuration for compliance with security standards.
Concurrent update	Two processes or transactions updating the same record almost concurrently. For example, the first transaction reads the opening balance and updates it. Before the first update, the second transaction reads the balance. The second transaction finishes after the first, and therefore overwrites the changes made by the first transaction. This is a database anomaly and can be prevented with record locking.
Control risk	The risk of an internal control being improperly designed, implemented or carried out.

Critical path diagram	It shows the planned elapsed time of predecessor dependent activities. The path of contiguous and predecessor dependent activities with the longest planned cumulative elapsed time is called the critical path. There is only one critical path in a project. A delay in the critical path will delay the project.
Cryptography	An area of mathematics that is applied to protecting data by scrambling. It can also be used to produce digital signatures to authenticate electronic messages and files.
Customer relationship management system	A system that uses data mining to find out who the valuable customers are or what turns on customers to lead to more sales. For example, many affinity card programs include customer relationship management systems.
Data anomaly	This exists when inconsistent changes to a database can be made. For example, when a customer moves, the customer address has been updated in some tables but not in others.
Data dictionary	A master table in a database that defines what data is in each table, the format of data, what programs and users have access to which field and the type of access, e.g., read or write. The data dictionary is used by applications to locate data in a database.
Data Encryption Standard	A common and old encryption algorithm using a 56-bit key. Considered to be insecure for eBusiness.
Data mining	Quantitative analysis of a large mass of data including transaction data and external data to determine patterns. This is commonly used in customer relationship management systems, risk analysis and executive information systems.
Data redundancy	Keeping repetitive data in a database that increases the risk of data anomaly.
Database	A logical collection of files with related or similar business purposes to facilitate sharing and correlation of data to enhance customer service and decision support, e.g., banks use databases to correlate customer business across types of services.
Database administrator	The person responsible for configuring and monitoring a database and the database management system.
Database management system	This is a system software tool that manages data sharing in a database by allocating data table access to computer programs and users.

Database synchronization	A database control to compare the content of copies of databases distributed over servers and networks to ensure they are synchronous including time synchronization.
Deadlock	An application coming to a halt as a result of multiple record locks that lock out contending transactions. The database management system has to be configured to detect this and then release all locks but the first one in progress in order to allow the affected transactions to be completed.
Defence in depth	Placing multiple layers of firewalls and intrusion detection systems in a network to successively protect inner servers and provide for redundancy.
Detection risk	The risk of audit procedures failing to detect a significant transaction error. For internal auditors, detection risk also means the risk of test procedures failing to detect a significant control deficiency.
Development library	A library of programs being used in peer testing. Peer testing is also called string testing.
Digital certificate	An "electronic business card" about a user or a web site that is used by the other party in an Internet connection to authenticate the user or web site.
Digital rights monitoring	Using technology like digital locks to prevent the copying of software and data, including the disallowing of browsing object code when a software package is used.
Digital signature	It is an encrypted hash of a message or file to allow the recipient to verify that the message or file was actually sent by the purported sender.
Direct cutover	Converting the old system to the new system in one pass, without any overlap between running the old and new systems. This is risky but the trend because of competitive pressure and advanced technology that enables operation to revert to the old system in real time if necessary.
Distributed computing	A system that splits processing between central servers, intermediate servers and remote workstations. An example is ATM.
Disaster recovery plan	A plan to ensure that the organization can resume operation of business critical systems in the event of a significant interruption of the data center.

DMZ	Demilitarized zone is the network space between an external firewall and an internal firewall. Medium sensitive servers that do not contain financial information can be placed there. It is created as part of defence in depth. Web servers are commonly located in the DMZ.
Domain name server	This is a server that is used only in an IP environment. It translates URLs to IP addresses.
EBCDIC	Extended Binary Coded Decimal Interchange Code is the data format of IBM Z series server.
Echo check	A receiving node sends back what it receives to the sending node for the sending node to verify accuracy of transmission. This is almost fool proof but expensive because it doubles the traffic.
Electronic data interchange (EDI)	Transmitting common business documents in electronic batches, e.g., purchase orders, because two organizations, using a common data format like American National Standards Institute (ANSI).
Electronic vaulting	Online transfer of data to a backup server without using computer tape.
Enterprise resource planning system	An integrated accounting system that updates multiple journals and ledgers based on one transaction, thereby minimizing paper, key entry and phone calls etc. It also enables comprehensive, real time enquiries. Common products are SAP and Oracle.
Entity relationship diagram	This diagram shows the relationship between entities and the cardinality of relationships. For example, the relationship between invoice and product number is many to many. This diagram is part of database design.
Environment	The hardware or network segment that holds a software library.
Error detection value	The amount of redundant data sent along with a transmitted packet that will be used by the receiving node to verify complete and accurate transmission.
Exploit	A worm written to exploit a security hole like a back door.
Exposure	Quantified risk in relation to the value of asset or information at risk, i.e., risk x materiality.

File integrity monitoring	Using hashing algorithms to check the change in file size change.
Firewall	A security device placed on a network to filter out unacceptable Internet traffic.
Foreign key	An alphanumeric field in a table that is the primary key in another table. A foreign key is a field that must not be blank in order to preserve data integrity. An example is the supervisor ID of an employee.
Gantt Chart	A time table for a project, in calendar form showing the tasks across time lines, people assigned to tasks, person days required and deliverables. The chart should also accommodate the display of actual progress vs planned progress.
Hardening	Disabling unnecessary services (features) and ports of an operating system or similar system software package in accordance with the organization's baseline configuration image to prevent system attacks.
Hash total	A control total of a numeric field that is neither an amount nor a quantity, taken at one point of a transaction cycle for a batch system and agreed to another control total of the same batch of transactions taken at a later point to confirm completeness of processing. This control is used in addition to or instead of batch total to catch offsetting errors. For example, the field totalled may be the account number. In a batch total, if a $100 check falls through the crack and another $100 check is input as $200, this error will not be detected. However, if the check number is also captured in a hash total, this error will be caught.
Hashing	The irreversible scrambling of data using an algorithm; commonly used in digital signature formation, password protection and data integrity checks. No key is required because a hash is not intended to be deciphered.
Honeypot	A trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.
Hot site	An alternate disaster recovery site that is available within an hour of notice. It has all the hardware, software, work stations and backed up data.
Index sequential access method	A database access method that uses an index like the table of content in a book to facilitate locating records.

Inherent risk	The risk of an undesirable event.
Intrusion detection system	A sensor or a server with appropriate software to analyze traffic that has gone through firewalls to detect potential intrusion for assessment by security specialists.
Intrusion prevention system	A sensor or a server with appropriate software to deny traffic that has gone through firewalls but that is determined to be part of a hacking scheme.
Investor Confidence Rules	This is sometimes called CSOX, Canada's rules that require public companies to certify internal controls to their provincial securities regulators.
IT governance	The oversight responsibility for the strategic management of the IT function and resources. IT governance should cover IT planning, organization, acquisition, implementation, delivery, monitoring and evaluation.
Job Control Language	The operating system commands and log for z/OS; z/OS is IBM's operating system for mainframes (Z Series servers).
Joint application development	This approach combines the user requirement phase with the system architecture and system design phases. Workshops are conducted to involve user representatives, system architects and system designers to design the system and architecture from a user perspective interactively.
Kernel	The kernel is the core of an operating system that directly controls the allocation of the central processing unit (CPU) functions and random access memory (RAM).
LDAP	Lightweight Directory Access Protocol is a modern protocol for managing and exchanging PKI directories.
MAC address	Media access control address is a hard coded serial number of a computing device, like a vehicle serial number, used to uniquely trace the activities of a device.
Message digest	A hash of a message which can be encrypted with the sender's private key to form a digital signature. If not digitally signed, the message digest can still be used to check transmission integrity, i.e., nothing lost.
Near field communication	Short range wireless transfer of data within 20 cm. This is increasingly used for mobile payments of small amounts.

.NET	The .NET Framework is a collection of software tools for Windows application development, allowing for programming language interoperability, i.e., a program can include instructions written in other programming languages.
Node	A network connection point like a router or a server.
Normalization	Reducing the number of fields in database tables to a reasonable minimum to avoid data redundancy and make the database more modular.
Object code	Computer programs that have been compiled from the programming language format to computer or machine language understandable to the operating system. Only object code can be processed by a computer for calculation and transaction processing. Object code is usually linked as one object, e.g., software that we download is in one .exe file, to form executable code.
Open source	Ready made programs in source code format available from vendors, trading partners or the IT community.
P3P	Platform for Privacy Preferences (P3P) is a security protocol for web sites to declare how they will use the information collected through a browser, in accordance with their posted privacy policy. For example, if a privacy policy says that the organization will not use a cookie to change a customer's data in the PC, the web server logic should be internally certified by the organization that it will not use a cookie for that purpose.
Packet	A fixed block of data transmitted over a network. A message is usually broken into several packets so each packet can find the fastest route to travel. At the destination, the packets are regrouped to form the message. A standard packet has 1,024 bytes.
Parallel implementation	Operating the old and new systems in parallel until the new system is stable. This system conversion method is more suitable to batch systems, where the disruption and inefficiency caused by parallel running are relatively low compared to online, real time system.
Parity check	Using the last bit of a byte as a check bit for the receiving node to detect whether any bits in a byte has been turned on or off as a result of bad communication or hacker interception.

Password cracking	A hacker using password hash tables or trial and error to hash a number of text strings to try to find a hash that is identical to the stolen hashed password, with the intent of determining the real password.
Patching	Installing a security fix from a software vendor, e.g., Microsoft.
Payload	The damage done by a virus or worm on a computer; in a way, like the punch line of a joke.
Payment Card Industry Security Standards	A set of security standards established by the Payment Card Industry Security Standards Council made up of major credit card issuers like MasterCard and Visa, that apply to merchants, financial institutions and IT service organizations that process credit card transactions electronically.
Penetration testing	A control procedure whereby an organization hires a consultant or assigns technical staff members to try to hack into the organization, to test the network security.
Person-in-the-middle attack	A hacker intercepts the exchange of public keys and replaces them with his or her key and then subsequently uses his or her key to decrypt intercepted emails.
Personal information	Sensitive information about a person provided by the person, e.g., my salary information in my bank.
Personal Information Protection and Electronic Documents Act	Canada's privacy act that applies to any business and not-for-profit organization that is not substantially funded by a government and where there is no comparable provincial privacy legislation applicable to the private sector.
Phased implementation	A risk based system implementation approach where selected functions will be turned on, and those corresponding functions of the old system will be turned off.
Phishing	An email trying to trick a reader to click on a link to provide login credentials or financial information.
Pilot implementation	Implementing a new system in a selected store or branch to test the water.

Ping	A Windows command that tells you if a host is reachable and alive. It sends a packet that asks the target computer to return a message saying it is actually there. It also tells you how long it took to get back. This is a common command for trouble shooting and hacking.
Port	A channel used by computers on a network to exchange information for a particular application; an example of an application is a network game. A port is analogous to a radio channel.
Post-implementation review	An independent review of a system development project at completion to assess the extent to which cost and benefit comply with the business case, the adequacy of signoff and documentation as well as the level of user satisfaction.
Primary key	An alphanumeric field in a table that uniquely identifies records, e.g., customer number.
Privacy	Confidentiality of personal information, to protect the information owner from having the personal information used inappropriately at the detriment of the information owner.
Private key	This is the one of the key in a key pair generated by an asymmetric encryption algorithm that is kept private in a user or a web site system; used to decrypt messages and compose digital signatures.
Production library	The library of programs actually used in transaction processing. This is the master and official version of the programs in a system.
Project sponsor	An executive who owns a system development project and will be accountable for the project's success. This is usually the system owner when the system is implemented.
Public key	This is the one of the key in a key pair generated by an asymmetric encryption algorithm that is released to other parties, for use to encrypt messages and decipher digital signatures.
Public key infrastructure	PKI is a set of policies, procedures and software to manage the public key directory and enable users and systems to use the asymmetric encryption method in an organization and with other organizations.

RACF	Resource Access Control Facility is IBM's add on security software for z/OS.
Radio frequency ID	A portable device that can be attached to a physical asset to transmit information about the asset using radio wave to a reader for recording in system. A common example is a toll road transponder. Another example is a tag attached to a pallet of soft drinks to keep inventory up to date.
Record locking	A database control to lock the field of a record to prevent it from being read by a transaction that intends to use the field's information to update the field or other fields in the record, when there is already a transaction in progress to update that field, to prevent the result of the first transaction from being overwritten by the second transaction.
Redundant data check	A method of transmission verification that involves sending extra data that is a derivative of the actual message for the receiving node to verify accurate transmission.
Regression analysis	Correlative analysis of a hypothesized dependent variable and one or more independent variables to estimate a relationship.
Relational database	A database whereby any 2 tables with a common key can be correlated. This is the most popular database model.
Residual risk	This is the risk remaining after implementation of internal controls. Residual risk is acceptable when the cost of the next control will exceed the cost of the risk to be mitigated.
Reusable code	Programs that can be reused in other applications, e.g., boundary checking or sorting.
Risk register	A corporate repository of inherent and residual risks segmented by business area indicating the risk owners, weights and ratings, to facilitate ongoing risk assessment.
Rootkit	A program used by a hacker to obtain root access to the operating system to bypass security.

Run-to-run control total	A control total for a batch system prepared and verified by the computer without human interaction. For example, the payroll system of General Electric updates work-in-progress of major manufacturing contracts. In addition to the payroll data sent to work-in-progress inventory files, the payroll system also sends control totals which are verified by the inventory systems.
Salt	Extra bits added by a password management system to a raw password to arrive at a more complicated password, to make it harder for password cracking.
Sandbox	An enclosed area in PC based operating system that does not allow access to local files and input functions, it is like an operating system within an operating system.
Sarbanes-Oxley Act	A United States Act passed in 2002 after the collapse of some big public companies like Enron. This Act was proposed by Senator Paul Sarbanes and Congressman Michael Oxley, to tighten financial control over public companies. The Act requires the CEO and CFO of a public company to certify internal controls that support financial statements to Securities Exchange Commission. It also restricts shareholders' auditors of public companies in performing non-audit services to their audit clients in order to maintain objectivity.
Secure Electronic Transaction	Under Secure Electronic Transaction (SET), a bank issues digital certificates to customers and merchants for the purpose of authenticating the merchants in credit card transactions. The merchant does not see the credit card number and the bank does not see the order information other than the amount. This method of online sales processing is not used in North America.
Secure Socket Layer	SSL is the encryption method used in eBusiness, using a 128-bit symmetric key generated by a browser and sent to the web site encrypted with the web site's public key.
Session ID	A session ID is an ID assigned by a web server to a user upon the user initiating connection with the server. It helps the web server to keep track of user activities for problem solving, customer relationship management and what a user has requested so the requested information can be provided to the right user and web site visit pattern management system.
Single sign on	Using strong authentication to allow a user to access a number of systems via a two factor authentication process. This enhances the efficiency of user authentication.

Sniffing	Unauthorized tapping of network traffic.
SNMP community string	A text string that acts as a password. It is used to authenticate messages that are sent between the management station like a server or a router and the device (the SNMP agent) like a workstation. The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. All devices assigned to a management station have the same community string as the management station's.
Software change management system	A system that keep track of the versions of programs during development, testing and in production. It keeps track of the approvals, updates and retrievals of programs in the development, test, user acceptance (staging) and production environments.
Social engineering	Using seemingly benign approaches to obtain information about one's identity or an organization's network in order to perform hacking.
Source code escrow	A source code escrow agreement involves placing the current source code with a third party. In the event of a contract breach or the developing vendor ceasing business, the user organization can access the source code to maintain the system. This applies to software development contracts where there is incomplete trust between the two parties.
Spear phishing	Spear phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.
Spoofing	Disguising one's IP or email address to mislead the message recipient or network monitoring system.
SQL injection	A hacking technique to put in SQL instruction in an eBusiness data input field, thus causing unexpected system functions.
SSID	The ID of an access point that has been configured in an authorized remote device to authenticate the device.
Staging library	The library that holds programs being used for user acceptance testing.

Standard image	An approved and consistent set of configuration that applies to all PCs and servers in the organization.
Storage access network	A network dedicated to performing and storing data backup. It is a cross-department, cross site network that processes the online transfer of data and provides the means for business areas to retrieve backed up data online.
String testing	Testing of several programs at a time by a peer programmer. This is the second phase of testing.
Switch	A network device that connects workstations to a server. Compared to a router, it has a much smaller operating system so logging and rules for connection are more limited.
Symmetric encryption	The same key is used to encrypt and decrypt. The two parties must trust each other and have a secret way to share the key.
System administrator	A system administrator is someone who controls a server. This is a critical IT position and must be rigorously controlled.
System integration testing	Testing the entire or the majority of a system together before implementation. This is done by independent testers who do not have other IT roles and it uses a massive data bank.
System software	Software that interfaces between the operating system and applications to perform common resource management functions like database management.
TCP/IP	Transmission Control Protocol/Internet Protocol is the Internet's protocol that allows seamless data transfer.
Threat	A general description of a risk without quantification, e.g., a snow storm.

Triple DES	A much improved symmetric encryption algorithm that uses three 56-bit keys in iteration to achieve an estimated effective key length of 112 bits. Why not 168 bits? Well, the iterations make it easier for hackers to deduce the keys and this compromise has effectively reduced the key strength to 112 bits. In general, Triple DES with three independent keys has a key length of 168 bits (three 56-bit keys). The first key is applied to encrypt. The second is used to decrypt the result from the first key. The third key is used to encrypt again. Obviously, the result of step 2 is not the same as the original plaintext. Because the second step is decryption, it compromised the combined key length so the effective key length is 112, not 168.
Trojan	A program that performs a useful function but also contains a hidden function that compromises security.
Two factor authentication	Using something a user knows and something a user has to authenticate a user, e.g., ATM.
User acceptance testing	Testing performed by user representatives to confirm a system's reliability and user friendliness, including the testing of user procedures. This is the last phase of system change testing. It focuses less on technical specifications than system integration testing but more on user satisfaction, although on based on written test expectations and results.
UDP	A simpler form of Internet communication than TCP. UDP uses a smaller header and does not check for errors. It is used when speed is more critical and internal data transmission is brief, e.g., finding out which computer has what IP addresses in an internal network.
Unit testing	Testing a program or several programs performed by the person who wrote the program(s). This is the first phase of systems change testing.
Virtual private network	Using encryption and two factor authentication to allow a user to access a corporate network via the Internet to protect data transmission and authenticate the user.
Virtualization	Using system optimization software to reallocate disk space and real memory in servers to maximize performance, thereby reducing the number of servers.

Virus signature	This is the "DNA" of a virus. It is a unique combination of bits in the virus. It is rare for two objects to have the same combination of bits. Thus a signature can uniquely identify a virus for detection.
Vulnerability	The extent of risk as a result of a control failure or absence, for example, an operating system is vulnerable if is not updated regularly.
Vulnerability assessment	An exercise whereby an organization's security staff reviews the network and operating system configuration to identify security holes, including where necessary, penetration testing.
Warm site	An alternate disaster recovery site that takes a day or two to be available. It usually has hardware and backed up data. But the software has to be brought up to date.
Web site refresh	Regularly refreshing a web site's content from a backup version to nullify any change by a hacker.
Wifi Protected Access	Wifi Protected Access (WPA) is the most secured encryption protocol for wireless access to a local area network. It complies with the latest IEEE (Institute of Electrical and Electronic Engineers) standard 802.11i.
Worm	A malicious program that travels on the Internet that will infect computers on the Internet or the same local area network where the worm is travelling. Typical damage is sending many packets of data to tie up the network. It does not require any action by a victim to infect a computer. The effective mitigation is to patch computers to prevent infection.
Zero day exploit	An exploit that is written to be a worm on the day a backdoor is publicized, thus leaving very little time for software vendors to react.