SOLUTION MANUAL

CHAPTER ONE

Review Questions

1. Which system component is the most business critical and why?
   The 5 system components are infrastructure, software, procedures, people and information. Even though information is often the result of computer processing, i.e., the end, it is the most important component of a system. 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.

2. How would you rank the system assurance criteria for a financial statement audit? For an internal audit?
   The assurance criteria are completeness, authorization, accuracy, timeliness, occurrence and efficiency. Financial statement auditors are concerned about completeness, authorization, accuracy and occurrence equally. They are less concerned about timeliness; if timeliness affects the year end, it becomes a completeness issue. Financial statement auditors are not concerned about efficiency. Internal auditors are concerned about all criteria with efficiency the least concerning; this is because it is better to have reliable information that took a lot of effort to get than to have unreliable information that took only a few minutes to get.

3. Computing power doubles annually. How do you think this affects system assurance?
   This allows organizations to collect, store and analyze more information. While that helps makes business more efficient and far reaching, it increases the risk of privacy intrusion, so the criterion affected is authorization in a potentially negative way. Authorization is also at greater risk as organizations increasingly empower their employees so employees have more direct access to systems and more tools at their disposal. The criteria that are favourably affected are accuracy and timeliness.

4. What are the criteria for assessing system criticality in a bank? A large retailer? A government?
   The criteria for business criticality in a corporation addresses mainly profitability (including revenue and expenditure control) and customer service. These apply equally to most industries. On a finer scale, the riskier areas in a bank are credit and cash management. The riskier area in a retail company is supply chain management including inventory. The criteria for a government include safety, health, welfare, revenue and expenditure control. The criteria for a university would include education, faculty support, revenue and expenditure control.

5. What is the IT implication of International Financial Reporting Standard?
IFRS implementation will lead to changes in accounting systems depending on the industry and the extent of computerization in an organization. For example, IFRS does not permit LIFO.

6. How can IT auditors be proactive to help manage risks?
An internal auditor can make recommendations to control deficiencies to help improve controls. The internal audit department should adopt a systems development audit methodology to mirror the organization's systems development methodology in order to review systems development documentation as it is prepared to identify potential control deficiencies. The internal audit department should also establish a protocol with management to review draft policies and procedures to help ensure that there are adequate internal controls. External auditors' proactive roles include testing internal controls during the interim audit and bringing control deficiencies to management attention ASAP.

7. What do you see is the role of a computer audit specialist in a financial statement audit?
As the general population is more IT literate day by day, so are auditors. Today's auditors can understand and test some IT controls that, twenty years ago, required computer audit specialists. Meanwhile, IT is growing and becoming more sophisticated. Hence, there is still a need for IT audit specialists. A computer audit specialist should be used to assess infrastructure and software change controls as they tend to be more technical, for medium to large organizations.

8. Which of the current IT issues identified in the CICA survey do you think affect the financial statement audit more?
A. Data integrity directly affects the control assurance criteria of completeness, accuracy, authorization, accuracy and timeliness and there is crucial to the external auditors. Information management to prevent overload and ensure that the right information goes to the right manager is of less concern for non-financial information..
B. Legislation, regulations and compliance – This is of high concern to the financial statement auditors because of the legal nature.
C. New and emerging technologies – This is of concern to external auditors because if new technologies are deployed without proper testing and training, transactions may be processed incorrectly.
D. Information skills and resources – This is of high concern to low to moderate concern to external auditors because inadequate knowledge can lead to incorrect transactions and inadequate staff can decrease segregation of duties.
E. IT governance – This is of moderate concern to external auditors because governance forms the platform for internal controls. The concern is moderate because the controls actually exercised by senior management are less directly relevant to transaction processing.
F. Outsourcing – This is of high concern to external auditors because it can affect their ability to test internal controls.

G. *Public trust – This is of moderate concern to external auditors because the lack of public trust means systems are not reliable..*
H. *Management and operation of technology infrastructure – This is of high concern to external auditors because they affect infrastructure controls, including general controls.*

I. *Business continuity and pandemic awareness – This is of high concern to external auditors because of the going concern relevance.*
J. *Impact of the economy on information technology – This is of a moderate concern to external auditors. The concern stems from deteriorating segregation of duties potentially resulting from economic downturns.*

9. Which components of the CISA examination do you think are more relevant to the audit of financial statements?
   The components are:
   A. *Information systems audit process – This is directly relevant to external auditors because an audit that requires an external audit usually relies significantly on information systems.*
   B. *IT governance - This is of moderate concern to external auditors because governance forms the platform for internal controls. The concern is moderate because the controls actually exercised by senior management are less directly relevant to transaction processing.*
   C. *Systems and infrastructure life cycle – This is directly relevant because it is critical for management to management the life cycles to ensure systems continue to be reliable.*
   D. *IT service delivery and support – This is highly relevant because unreliable service delivery and support will lead to incorrect transaction processing.*
   E. *Protection of information assets – This is highly relevant to external auditors because inadequate information asset protection will lead to unauthorized or unsubstantiated transactions.*
   F. *Business continuity and disaster recovery – This is relevant because of going concern.*

10. What kind of IT knowledge do you expect of the chief auditor of a large bank?
    A large bank has extensive information systems so it is important for the chief auditor to be IT savvy on a wide scale and keep in touch with IT deployment in the bank. S/he has to be an IT generalist that is willing to learn from conferences, discussions with staff and meetings with IT executives. The chief auditor should be IT literate enough to have regular meetings with the chief information officer to assess IT risks at a corporate level.

CASE

1. What do you think are the causes of aging systems in the public sector?
   Governments have experienced funding constraints in recent years as a result of increasing public demand for services and decreasing tax revenues. This puts pressure on the IT budget. It can lead to a general attitude of keeping systems until they break, even if they are aging and require more and more patching. Patching (maintenance and fixing of source code) for functional reliability and efficiency, is risk and error prone in general.

2. Are the causes of aging systems applicable to the public sector also common to the private sector?
   These factors are also applicable to the private sector especially for companies with legacy systems that are not essentials. Companies that experience revenue contraction will have to cut expenses. Unlike governments, companies are more inclined to cut people instead of IT budget because efficient and reliable systems make them competitive.

3. How do the risks of government systems differ from private sector business systems?
   The risk factors of completeness, accuracy, authorization, timeliness, occurrence and efficiency apply to both the private and public sectors. Private sector organizations are more concerned about efficiency and timeliness than public sector organizations.

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 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
E. Efficiency

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

1. How does automation affect segregation of duties?

   Automation usually reduces the number of employees in a process. This means less segregation of duties. However, one might argue that some duties formerly carried out by people are now automated. Since computers don't lie or collude and seldom makes mistakes, even though there are fewer people left, segregation of duties has not suffered. Well, that is a misconception, because in thinking so, one has neglected the fact that computers are controlled by people and therefore people can use computers to collude. Thus, we are back to the initial assessment that automation reduces segregation of duties and that is generally the case.

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

   The chief risk officer should also 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 registry, 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.

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

   Because of portability, the biggest risk faced by ATM users is the risk of unauthorized transactions. Unlike the risk of inaccuracy, incompleteness or untimeliness which can be prevented with system functions, the risk of unauthorized transactions can be magnified by users not safeguarding their cards and PINs properly.

4. Why are financial statement auditors content with moderate control risk?

   Because the purpose of the audit of financial statements is to express an opinion on the fairness of the financial statements, rather than an opinion on controls, the level of control assurance sought by the external auditors is only moderate. This moderate level of assurance limits the extent of control testing conducted by external auditors. This is why external auditors typically use smaller sample sizes when testing controls compared to internal auditors. In fact, external auditors often rely on the work of internal auditors to further limit the extent of control testing conducted directly. Such reliance will help to keep the audit fee low.

   When the external auditors can conclude that internal controls are moderately reliable, they can limit the scope of their substantive testing, i.e., the testing of transactions and account balances for substantiation. Substantive testing is generally more time consuming than internal control testing so it pays for the external auditors to seek a moderate level of internal control reliance. For

example, if the external auditors can conclude that internal controls over credit granting and sales processing are reliable, they can limit the scope of account confirmation and vouching to sales and payment details for substantiation.

5. What is the relationship between sample size and risk?

   Both control testing and substantive testing involve sampling. The larger the sample size, the more likely that the sample result will reflect the state of population. Therefore, there is an inverse relationship between sample size and risk.

6. What level of control risk can external auditors tolerate when giving an opinion on a client's compliance with Sarbanes Oxley Act?

   Sarbanes Oxley Act requires a public company to file a report with Securities Exchange Commission that includes an external audit opinion on the adequacy of internal controls that support the financial statements. This opinion is in addition to the external audit opinion on financial statements. Because there is now an opinion on internal controls, the control risk tolerable to the external auditors is low.

7. What risks do consultants cause to an organization?

   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.

8. What computer characteristics can both increase and decrease risk?

   Computers are fast so the risks of untimeliness and inefficiency go down. However, computers can also make mistakes fast and magnify financial loss if programs are wrong. Computers are consistent so there are few mistakes; they don't get tired. But computers are inferior to people in making judgements. Computers can store a lot of data so the risk of incompleteness goes down, but at the same time, a vast quantity of data can be accessed within a short time so the risk of unauthorized access goes up.

9. Referring to the top ten IT issues in Chapter One, which ones increase financial statement risks?

A. *Data integrity directly affects the control assurance criteria of completeness, accuracy, authorization, accuracy and timeliness and there is crucial to the external auditors. Information management to prevent overload and ensure that the right information goes to the right manager is of less concern for non-financial information..*

B. Legislation, regulations and compliance – This does not directly affect the risk of misleading financial statements in term of financial balances. The risk has to do with adequate disclosure of contingent liability resulting from failure to comply with legislations and regulations.

C. *New and emerging technologies – The use of new and emerging technologies may lead to incorrect transactions if the systems or tools have not been properly tested or if users are not properly trained.*
D. *Information skills and resources – The risk relevant to financial statements is inadequate knowledge, which can result in incorrect transactions.*
E. *IT governance – This is a risk for financial statements because governance forms the platform for internal controls. The concern is moderate because the controls actually exercised by senior management are less directly relevant to transaction processing.*
F. *Outsourcing – This is a significant risk for financial statements because it can affect their ability to test internal controls.*
G. *Public trust – This risk has to do with systems used by the public. The lack of public trust means systems are not reliable so that means financial statements are not reliable.*
H. *Management and operation of technology infrastructure – The financial statement risk implication is high because improper management can lead to weak infrastructure controls, including general controls.*
I. *Business continuity and pandemic awareness – This is irrelevant to the financial statements but relevant to the audit opinion because of the l going concern issue.*
J. Impact of the economy on information technology – This is a moderate risk. The concern stems from deteriorating segregation of duties potentially resulting from economic downturns.

10. As an internal auditor, you have been asked by the CIO to develop a risk registry. How should you respond to this request?

Risks are owned by management and they should document risks and mitigation plans. Auditors can review the risk documentation and provide comments. Auditors can also provide input as requested before documentation is finalized and can even participate in working sessions as an advisor; but auditors should not develop risk documentation.

CASE

Audit Planning Memo
To: Audit Partner
From: Junior Auditor
Re: Automotive Parts Incorporated (API)

I have analyzed the information provided on API, a returning audit client, and the following is my analysis.

Automotive Parts Incorporated (API) is a distributor of automotive parts. Its customers include service shops and retailers. At the beginning of the current fiscal year, the company had implemented a fully electronic sales system that includes order entry, invoicing, receivables and collection. This system connects the head office with 5 branch offices with a wide area network (WAN), where each branch has an individual warehouse. This new electronic system will increase our overall audit risk because as a new system, our auditors have never been exposed to it and tested the strengths of the system controls and effectiveness. Therefore there is a high level of inherent risk for this audit. The transfer of information from previous systems to this new system will also have a high propensity for errors. This system will be one of the primary focuses of our audit because it can affect many important figures on the financial statements such as accounts receivable, sales and inventory. The audit will be designed around testing the controls that exist within the system as well as conducting several substantive tests in areas where controls are weak.
The following is my analysis of the issues that have been provided as well as my suggestions as to the audit approach to address the issues.

Issues Identified:
Issue 1: In API's organization, the information technology (IT) manager reports to the CFO. There is a computer operations supervisor at head office and one at each branch. They report to the IT manager. They are specialists in operating systems and networks. In addition, they have been thoroughly trained in the use of the application software packages purchased by API.

Inherent Risk: There is always an inherent associated with multiple points of entry into any system. Multiple points of entry increase the chance of fraud or error. However, inherent risk may also decrease given that those given access are properly trained. It also decreases because there may be an increased chance of detection of any system errors.

Detection Risk: This memo is prepared using the information provided by the CIO. However, based on the above information provided by the CIO, the direct user of this system is not the CIO but the computer operations supervisor at each branch and head office (See Appendix). Therefore, there is a risk that as auditors we are not provided with the complete image of this system.

Control Risk: There is a computer operations supervisor at each location whom are all well trained in the use of the application software. This decreases control risk because these supervisors, through their continuous exposure to the system would be able to detect system errors more easily than other employees. They would also be able to correct system errors before the error expands. Therefore, these supervisors serve as an added layer of control against system errors that might lead to material misstatements of financial figures. The IT Manager would also serve as an oversight control to ensure that no changes are made without proper authorization.

Audit Approach:

Completeness: Assurance needs to obtained in regards to the information that we as auditors have been given by the CIO is complete. In addition to the information provided by the CIO, our audit team needs to approach each computer operations supervisor and the IT Manager for additional information and concerns they have about the system. Method used to obtain information can be through individualized interviews.

Authorization: Additional information should be obtained in regards to how these supervisors obtain their access to the system. Through interviews, we should also understand whether the supervisors have authorization to make changes to data on the system or to the system itself. If they do, how are they monitored to ensure that they do not make inappropriate changes? Also, their access should also be secure to ensure that no one else can access the information.

Existence: Whether these supervisors have actually been trained adequately in the usage of this software system should also be verified to ensure that this control actually exists. Auditors can observe the supervisors and ask detailed questions concerning the system during the interview process.

Issue 2: A service shop or small retailer customer that wants to establish an account would access API's web site to complete a credit application. Besides the standard information normally associated with a credit application, the applicant must provide a valid credit card number or bank account number that will be charged for all purchases. The customer must also supply an email address.

Inherent Risk: Electronic commerce in general increases inherent risk because third parties are responsible for data entry into the API's system. Customers are not data entry experts, therefore information provided in reference to name and email address may be incorrect or entered in an incorrect format. For example, the usage of "-" in the entry of phone numbers and usage of brackets are preferences that differ among different individuals. This can be linked directly to a higher detection risk for audit company if not properly controlled.

Control Risk: The system requires that the customer provide a *valid* credit card number or bank account number, which suggests that the system picks up anomalies in those data fields immediately upon entry. This decreases control risk, as the system will guarantee that the account exists before any purchases can be made. Since this is a low control risk, it is one of the key controls that can be relied upon in the audit procedures.

Detection Risk: Detection risk may increase due to the inherent risk of having third party users of the system. For example, as auditors, we frequently use CAAT systems to run through the data provided by the company in order to detect anomalies in the data. If the formats of the entries are all different, then using the CAAT, we may have a long list of anomalies that were simply the result of the customer adding dashes or brackets in the phone numbers and not actual incorrect entries.

Audit Approach

Existence: One of the key assertions that we have to test for is existence of the customer provided information, given that mistakes can be made in data entry. However, as we have stated earlier the data field control can be relied upon. Therefore, the auditor should first test the controls by running a CAAT to enter various credit card numbers that do not exist into the computer system and ensure that the system does not accept these numbers. As a precaution, we may also want to take a sample of bank account numbers and verify with the bank that these accounts do exist.

Accuracy: To ensure that the data entered by the customer is accurate, a sample of the customers could be contacted and asked whether the information in the system is accurate. Banks can also be used as a external source to ensure bank account numbers match customer names.
Completeness: CAAT could be used to pick up customer profiles that have important fields missing or incomplete.

Issue 3: The applicant's credit status is verified electronically with a credit rating agency, and the API credit manager approves the applicant as a customer within two business days. Upon approval, the customer's system ID and password are sent by separate registered letters. A customer can use the ID to access API's order entry web site.

Inherent Risk: The inherent risk or any non-automated system is the risk of human error. On the other hand, the inherent risk of automated systems is that they lack human judgment. One system glitch may cause many customers to be approved even though they have lower credit rating before it is detected. However, the additional API credit manager approval is an added measure to mitigate this inherent risk. However, as stated previously, systems are not biased nor do they make mistakes. By having the API manager in the process, there is added inherent risk of biases, fraud and human error.

Control Risk: There are multiple control factors here. The applicant is not given access to the website online purchasing system until after their credit rating have been approved. This decreases collection risk for the client because customers are more likely to be

trustworthy. This can be directly tied to our auditing of the accounts receivable on the financial statements. The number of bad debt expense for customers that purchase through the website might be considerably lower than previous years. With automated systems there are always an inherent risk that a malfunction may not be easily detected. In this case customers with bad credit rating may be accepted. However API added a human verification process by using a credit manager to approve of all customers before they are sent their passwords and system IDs. This means that system errors may be noticed more quickly and adjustments made. This decreases the control risk. The customer's ID and password are also sent through separate letters. This ensures if a letter gets intercepted or opened by another person, they would not have the complete information to access API's online website.

Detection Risk: One particular issue that may be problematic for auditors is that there may be difficulty in ascertaining whether the system functioned correctly when it was verifying the credit risk of a potential customer. Credit ratings for customers can change overtime. Therefore, if the credit rating agency does not keep a record of historical credit ratings, it may be difficult for auditors to conduct accuracy assurance testing to ensure the system rejected the appropriate customers.

Audit Approach:

Accuracy: The system automatically verifying with a credit agency is a key control that can be relied upon in our audit. Therefore control testing becomes imperative. The credit rating company should be contacted with a selection of customers to match their ratings and ensure accuracy. A potential weakness of this system is that it may not update consistently when there is a negative change in the credit rating of a customer. This might mean that collection risk may still be an issue for the company.

Authorization: To test the control of the credit manager having to approve all new clients, a sample of recently approved clients should be selected and the approval of the credit manager should be verified. Another authorization issue is the dual mailing of the ID and password. This control is not a key control as it is subject to much risk. Both letters can be mailed to the same wrong address. They could both be intercepted. Therefore, more details as to how this dual mailing process would actually help maintain confidentiality and ensuring that no unauthorized person obtains the ID and password would have to be known. A suggestion could be made to management to send ID electronically through email. When customer obtains ID, they can enter the website whereby they provide the ID plus additional personalize information that the system could match up to customer profile and then the password will be sent to the customer.

Issue 4: Using the ID and password, a customer can look up product availability at any of API's five warehouses and place an order.

Inherent Risk: There is inherent risk in fraud from identity theft as unauthorized individuals might steal customer's information and misuse their accounts. Moreover, customers will expect the information on the product availability at the warehouses to be

both accurate and timely. Inherent risk arises as the information might not be accurate and customers might end up ordering products with no availability, thus, creating an error. This is evident through a later issue where warehouses have to sometimes fulfill orders for items that have been ordered from another warehouse. This particular risk is more of an important issue from internal auditors as it has a direct link to efficiency and transportation costs for the company. As external auditors, our concerns would be whether these internal transfers are properly accounted for as shipping costs. Another issue is the inventory count as products can be easily double counted if they are shifted between the warehouses. The transfer of inventory between warehouses effectively demonstrates that the system is not timely and consistently accurate on product availability. Therefore, this inventory count on the system itself cannot be relied upon by our auditors.

Control Risk: The ID and password only provide sufficient control to ensure proper authorization and low control risk in frauds if they have a high degree of security and cannot be easily guessed or attained by a third party. However, assuming that the password and ID is secure and customers have no access to the system aside from making orders, the security aspect of this internal control should be relied upon as it has a significantly low control risk, but should be tested to ensure reliability.

Audit Approach

Authorization: The ID and password system can be tested by sampling customers with positive confirmation by phone to ensure these orders have been properly authorized by these customers.

Accuracy: Accuracy pertains to the amount of inventory in the warehouse to the numbers entered into the system by the warehouse staff. This can be tested by sampling the warehouse to compare the amount inventory available and the number in the system. This assertion should be given greater caution as it is prone to human error in the inventory count.

Timeliness: Timeliness pertains to the number entered by the warehouse staff and the number that appears on the product availability online. This can be tested by sampling the numbers on the website and the numbers on the internal inventory system. This can effectively test whether the internal inventory system data are fed timely to the website's product availability counts to ensure timeliness of the data online.

Existence: For the inventory count, existence will be a major concern as the system does not update automatically. At the cut-off period year-end, it will become empirical to identify the exact amount of inventory in the five warehouses. The system as previously stated cannot be trusted to have the accurate amount. Auditors would have to use inspection of the five warehouses as well as look into shipping papers in order to determine the exact amount of inventory.

Issue 5: For small customers, when a customer finishes placing an order, API's system connects to the previously identified bank or credit card network that will authorize the transfer of funds, to ensure that sufficient credit or cash on deposit is available. API records this code on an electronic order confirmation that has a unique order number assigned sequentially by API's computer to every order placed within its system. The order confirmation and invoice are emailed to the customer. Large customers are invoiced and they will pay based on the invoices.

Inherent Risk: For small customer, an inherent risk to the process is the accuracy of the e-mail provided by the customer. If the e-mail is not correct, the billing process could not be completed and the customer could not be notified for their payment. In addition, there is inherent risk in billing incorrect amount or incorrect account and possibility of billing to accounts with insufficient credit. For large customer, similar risk exist as the billing address and amount or account billed may be incorrect and the account might not have sufficient credit. Lastly, there is the inherent risk that some orders might not be billed.

Control Risk: There are controls in place to ensure the amount billed and the accounts billed to be correct and has credit available for the billed amount. Moreover, the billing information is controlled with sufficient system edit in place to ensure the validity of the information provided by customer upon their registration. Our recommendation would be to rely upon these controls as the control risk is low. However, as key controls they would need to be tested extensively to ensure that the system is functioning properly when it seeks to determine whether the client has enough credit and when it sends out order confirmations to clients.

Audit Approach

Existence and Accuracy: The amounts billed and accounts billed can be tested by sampling the invoices sent out to the customers and comparing to the original order received to ensure that the proper amount and account have been billed.

Completeness: To ensure all orders received have been billed, the billing record and order record could be compared to ensure that all orders have been billed with an invoice. Also, using a CAAT system, the auditors should test for whether there are duplicate order confirmation numbers and whether there are any missing sequence numbers.

Issue 6: For small customers, funds are electronically transferred to API's bank account one week after an order has been filled, to allow customers time to inspect goods before paying for them. The customers have the right to cancel the transfer of funds by informing the bank if the goods are not satisfactory.

Inherent Risk: There is inherent risk in the transfer of fund, whether or not the proper amount have been received from the proper account. Moreover, there is inherent risk in the cancel of the order, as customers might miss the 7 days deadline to cancel the transfer of fund. There are also inherent risks with allowing customers time to cancel the purchase of goods after the goods have already been shipped. The revenue recognition policy of

API should be observed to ensure that they do not recognize revenue prematurely as the risk is high that the customer may not accept the goods. Also, cut-off becomes an issue as the inventory goods would have left the warehouse but are not yet effectively sold to the customer. This risk will lead to an increase in detection risk as it can be difficult to determine which customers will keep the products and which will not. Also, if customers are widespread it becomes difficult to substantively test for the amount of inventory not currently in the warehouses.

Control Risk: There is an automatic system in place to transfer the amounts electronically. This greatly reduces the chance of human error and should be relied upon. However, it should be tested to ensure the system is reliable. In the case of a canceled transaction, fund would still be transferred if customers did not notify their banks. Thus, this should be tested in detail to ensure that there is no additional funds received for cancelled orders.

Audit Approach:

Accuracy and Completeness: The automatic system can be tested for its accuracy and completeness by a bank reconciliation. In addition, the bank reconciliation can test whether additional funds had been received for the cancelled orders.

Issue 7: During the day, the branch system processes transactions in "memo mode" only. "Memo mode" means that the branch's own inventory data base is updated instantly but that the transactions are not yet processed or transferred to the master files in head office. Orders are updated to the corporate system overnight.

Inherent Risk: the automation of updates will decrease inherent risk as it eliminates the possibility of human error when updating the database. In addition updates from the local branch to the corporate system occur every night. This systematic update of the files will decrease inherent risk as it is much easier to find errors between the branch database and corporate database due to systematic update. On the other hand inherent risk increases because of the timing of the updates of the master files. Since master files are not updated immediately in memo mode, there is an increased inherent risk of error between the timing of the updates. In between the updates of the local branch data base and the corporate master file, there is room for users to change information in the local database before it is updated. In addition, the corporate system will not be updated throughout the day, this may lead to customers ordering inventory that has already been sold to other customers.

Detection Risk: having electronic paper trail will allow CAATs to operate efficiently and detect errors easily thereby decreasing detection risk. However, having a completely electronic paper trail will increase detection risk as well. Without a physical paper trail, some transactions may be undetected or easily covered up if it is not recorded electronically.

Control Risk: automation of the updates of the local data base to the corporate master file reduces the control risk associated with this process. It limits access to the files to prevent potential fraud or misstatement by a third party as the system will automatically update itself without. However, the lack of authorization to approve of updates of the local inventory data base to the corporate master file increases control risk because no one checks over the files that are sent to the corporate system to make sure they are correct.

Assertions

Completeness: One of the key assertions is to test for completeness. Auditors should perform a test of detailed balances by comparing the sub-ledger to the general ledger to make sure the local database matches master file. In addition, a sample of the update file can be taken to check if all transactions from the branch database goes to the corporate master file.

Accuracy: to ensure the master file is accurate, a sample of various local data bases should be taken and compared to the master file to ensure the balance from the local data base matches that of the master file.

Issue 8: Each evening, the network supervisor at each branch performs an end-of-day routine that identifies every transaction processed that day. The routine writes these transactions to an overnight transfer file. At the end of the daily update, head office sends a complete copy of all updated data files so that each branch has current customer, item number, order information and inventory levels at all branches.

Inherent Risk: by having the network supervisor identify each and every transaction processed that day, there is a high probability of human error and fraud which increases the inherent risk. For example, the network supervisor can record a transaction incorrectly, fail to include some transactions, double count transactions, or add false transactions. In addition, the quantity of the processes from the routine to the transfer to the head office and the update back to the local office increases the inherent risk as it allows for more room for misstatement at each stage of the process.

Detection Risk: the updated file sent to all branches from the head offices creates a paper trail that is frequently updated. This will decrease the detection risk as it gives auditors a paper trail to trace transactions that occur at each branch and compare it to the corporate master file.

Control Risk: by having only one person compile the report on every transaction processed in the day there is a lack of supervision and authorization over the routines. There is a lack of segregation of duties as well since this allows one person to include or not include transactions of his choosing in the report without supervision. As a result, the controls in place are not adequate and will increase control risk

Assertions

Existence: existence can be tested by taking a sample of the report on the end of the day routine at various branches and compare it with the master file at the head office. This can verify that the transactions have been recorded at both the branch database and corporate master file. In addition, sample transactions from the report on end of day routine can be taken and verified with branch managers or clients to ensure transactions have occurred.

Completeness: Completeness can be tested by performing a test of detailed balances to make sure the inventory levels and order information match at both the branch database and head office master file. CAATs can also be used to sure all transactions from the branch database go to the corporate master file as well.

Issue 9: Three types of packing slips are printed every morning from the updated file. For example, the three types of packing slips printed at Branch A would be:

- *Sales to Branch A's pre-assigned customers filled by Branch A's warehouse*
- *Sales to other branches' pre-assigned customers filled by Branch A's warehouse,*
- *Sales to Branch A's pre-assigned customers filled by other warehouses.*

Inherent Risk: the three types of packing slips increase the inherent risk as there is a human error aspect. The possibility of mixing up the packing slips and sending packages to the wrong customers or losing packing slips after they have been printed out are all human errors that may occur in the warehouse after printing the packing slips. In addition, printing the packing slips in the morning does not allow for updates to orders made last minute or updates to orders that are to be shipped later but have the printing slip already printed out. As a result, this will increase inherent risk

Detection Risk: the three types of printing slips provide a paper trail that can easily be used by auditors to detect. However, the constant movement of inventory (e.g. sending inventory from warehouse A to warehouse B customer, and vice versa) has the potential to create mass confusion between each branch's warehouse and matching the inventory to a particular sale. There is the possibility of double counting inventory already assigned to another branch customer or not counting inventory that are in traffic from one warehouse to another. As a result it will increase detection risk because it makes it very difficult to keep track of inventory between the branches.

Control Risk: there is a lack of control as no one checks over the packing slips when they are printed or checks the proper packing slip is assigned to its package. This can create errors with sales as no one verifies accuracy of the packing slips and allow employees to steal inventory as employees can discard packing slips and steal inventory that was to be shipped from the packing slips. The lack of authorization and proper sign off for the packing slips increases control risk.

Assertions

Accuracy: a sample of shipped packages can be verified with packing slip to ensure accuracy of shipment. In addition, printed packing slips can be compared with the sales orders on database to ensure sales orders are correct and match the system database

Existence: physically sampling packages to ensure they are properly classified and going to the correct customers can be used to ensure existence. In addition, contact with the customers can be used to verify that the orders were received, all parts from the order were received and which warehouse the order was sent from.

Issue 10: Using hand-held computers, the shipping clerks scan the bar-coded shelf labels and enter the quantity they ship using the numeric keys.

Inherent risk: There is a high inherent risk in this manual process of scanning each item been shipped as there is always a high risk of human errors associated with manual data entry. First of all, as the client's main business is inventory, keeping track of inventory is always a high-risk area. This is especially the case for API as their inventory is automotive parts which can come in all sizes and value. A small part can be worth a significant value. Thus, having to scan each part that has been shipped, there is a risk of something not been scanned properly, missed or scanned twice. This can be linked directly to a higher detection risk for Audit Company if not properly controlled. For example, to test if all items on a customer's order are correctly shipped, audits might do a CAAT run to pick up any items that are on the customer's order but did not show up on the list of scanned items by the shipping clerk. This list will only show items that were supposed to be shipped, but not correctly scanned. It will not however show any incorrectly shipped items that were not on the customer's order list and not scanned correctly by the shipping clerk. Also, the quantity of the shipment also needs to be entered manually. This inherent the risk of human error as quantities can be entered incorrectly.

Control Risk: This process of keeping track of shipments requires the shipping clerk to scan each item with the hand held computer and enter in the shipment quantity using the numeric keys. This means, given all shipment is scanned correctly, any inventory that does not belong to the shipment should be alerted to the shipping clerk through the hand held computer. However, there is no control to ensure all shipment is scanned correctly and no item is missed. Because if an item is missed, there is no other control to alert the shipping clerk that an item is not scanned or does not belong to the shipment. In addition, there is no control to ensure that the quantity for shipment is correctly entered using the numerical keys. This increases control risk, as the process cannot guarantee the accuracy and completeness of the shipment orders. Since this is a high control risk, it is one of the key controls that cannot be relied upon in the audit procedures.

Audit Approach:

Existence: One of the key assertions that we have to test for is existence of each shipment, given that mistakes can be made in data entry of the quantities shipped and scanning. Because we cannot rely on control, there will be relatively more substantive testing to be done. To test if shipments exist, we can take a sample of customers and send out positive confirmation letters to verify the quantity and value of their order and whether they have been correctly shipped. We can also reconcile the electronic shipping record to the general ledger. We can also do analytical procedures by trace inventory movement with CATT and predicting the level of inventory that should be shipped.
Accuracy: We will need to reconcile the list of items prepared for shipment to the electronic recorded of items that is been scanned and shipped. To ensure that the shipment items scanned and entered by the shipping clerk is accurate, we can also take a sample of customers and send out positive confirmation letters to verify the quantity and value of their order and whether they have been correctly shipped. A random sample can also be taken from the orders of items that are going to be shipped and test if they have been scanned and recorded correctly by the shipping clerk.

Completeness: We need to reconcile year-end inventory and see if the quantity of shipment matches the associated decrease in inventory in addition to the testing we have done above.

MC 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 audit risk
c) Inherent risk x control risk
d) Control risk x detection risk
e) 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
e) Data loss

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.
e) The spreadsheet cannot be printed properly.

9. Outsourcing increases
a) audit risk.
b) control risk.
c) inherent risk.
d) detection risk.

10. When the shareholders' auditors find that internal controls are less reliable than expected, they should
a) assess control risk as lower.
b) increase materiality.
c) reduce the planned detection risk.
d) assess inherent risk as higher.

CHAPTER THREE

1. What is the relationship between software change controls and systems development controls?
   Software change controls apply to all software changes regardless of the size of a change. A system development project includes software changes. Some systems development controls depend on software change controls. For example, the validity of testing depends on the rigour in controlling software versions to ensure that tested programs are not changed without going through further testing.

2. Who should approve the corporate disaster recovery plan?
   Even though disaster recovery requires a lot of IT resources, IT exists to enable business so the DRP should be approved by management and the CIO. The corporate DRP applies to the entire organization so it should be approved by the organization's head, i.e., the CEO.

3. How often should a disaster recovery plan be tested?
   Many application supported by a DRP are business applications that have a maximum financial cycle of one year. Therefore, a DRP should be validated and tested at least annually.

4. Who should the CIO report to?
   The IT department is a common service function in an organization. To ensure that IT services are equitably distributed among other functions, the CIO should report to a senior corporate person. The most impartial senior corporate person is either the CEO or the COO. Ideally, the CIO should report to the CEO to show to the rest of the organization that the IT department is a highly valued service that should be used effectively.

5. What is the best approach to moving software to the production library?
   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 library as well as the 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 should reside 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 compared 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.

6. What is the difference between an environment and a library?
   An environment is the hardware that holds a library. A library is a collection of programs at a certain stage of development or in operation. For example, there are programmer library, development library, test library etc. There are also programming environment, development environment, test environment etc.

7. What does an auditor see in an organization chart?
   An org chart defines who reports to whom and what the job titles are. These two pieces of information allows an auditor to assess segregation of duties.

8. What is the drawback of parity check?
   It does not detect offsetting errors. For example, if a 1 bit becomes a 0 and vice

versa, parity check will not detect these 2 errors will lead to a wrong information being transmitted.

9. How often should a bank back up its transaction files and why?
   Banking is a highly online and time sensitive business. There is often no paper trail and also a bank cannot afford lose a transaction as an individual transaction could be huge in amount. It is critical for a bank to back up its transactions frequently throughout the day. In fact, a bank should use redundant servers to record every transaction at least twice in distant locations.

10. What kind of system is the grandparent-parent-child backup approach used for?
    Grandparent-parent-child backup method requires keeping at least 3 generations of a master file. This is more suitable for batch applications where the master files are updated daily. It is not suitable for online systems where the master files are updated continuously, because in this case, 3 generations of a master file may mean, at the extreme, only the updates by 3 transactions. That would be inadequate.

CASE – Progressive Realtor

To: President and Manager of the Information Services Division
From: IT Audit Advisor
RE: Control of activities in the Information Technology Division

After performing a thorough analysis of the activities in the Information Technology Division at Progressive Realtors Ltd (PRL), I have noted a number of weaknesses in the department's internal controls:

1. Organization of Controls

I would like to start my analysis with the company's organization of controls. It is important to ensure that information technology practices are consistent throughout the organization. Based on my review of PRL's activities in the Information Technology Division, I have several concerns:

(1) I & IT Strategy

The first issue, with regards to organization controls, that must be addressed is the alignment of the company's IT strategy with its business strategy. As I'm sure you're aware, Mr. Chow operates independently of the rest of the organization with minimal input from other managers. It is therefore important to review whether the IT department's functional strategy is congruent with that of PRL's overall business strategy. The implementation of a congruent IT strategy should include a description of the importance of IT and the organization's dependence on. The strategy should include how the development of the IT function will foster growth within the organization and

what specific projects and methods will be used to facilitate growth. Due to the fact that IT encompasses 15% of the company's total expenses, a proper approach to managing the investment and operations of this function would be important. The investments may need to be handled by a separate individual or a specific project-oriented budget may need to be prepared in order to ensure that investments are sound.

(2) IT Governance

IT governance controls help to ensure accountability. The same parties accountable for corporate governance should be accountable for IT governance. This means that Billy Chow should have the support of other executives in carrying out the company's IT governance framework. If necessary, an IT steering committee could be implemented in order to set the IT strategy and further approve major IT projects. Furthermore, a defined organizational reporting relationship should be established between Mr. Chow and perhaps you, the president of the organization, in order to ensure that information is transferred on a timely basis. This will be an effective control as it will not undermine the resources of the IT department and Mr. Chow's decision making abilities. By implementing a clear cut IT strategy, performance indicators and drivers of the IT department's performance can be established and can be better communicated to the executives of the organization. Functionality mapping and developing clear goals for each sector will ensure a proper consistency between PRL's operations and its IT strategy. In addition, it will aid with assessing the gaps between the operations of the IT department and those of the rest of the organization.

(3) Staff Development Controls

Staff development controls and procedures need to be established in order to ensure that PRL's Information Services Department continues to only employ only the best IT professionals. This could include hiring practices that clearly identify the specific skills and attributes that successful candidates should have. I would also recommend further training in order to ensure that the translation of data to an auditable format is accomplished.

(4) IT Budget Certification

Certification that the budget is adequately being utilized for IT procedures should also be a concern for the organization. Such procedures could involve the execution of budget review practices and better supervision of the IT function.

2. Segregation of Duties

Ensuring proper internal and external segregation of the IT function can help to establish proper accountability standards within a firm. As it stands, I have a few concerns with the segregation of duties at PRL:

(1) Segregating IT from Other Functions

First of all, the organization effectively separates the IT function from other corporate functions. More specifically, as I observed, Mr. Chow's team of workers primarily focuses on the programming, testing and maintenance of a number of information systems.

(2) Segregation of IT Function

While the IT function is satisfactorily segregated from other corporate functions, there is little segregation of duties within the IT function itself. There should be separation of systems development and systems operations. This means that the department's programmers and analysts should not be collaborating with system administrators when they are unable to interpret instructions or are on break. This area should be adequately staffed. Furthermore, the programmers/analysts should not be working with TREB and ASP customers online to troubleshoot any problems that arise since this is an area of operations not development. The separation of these functions would mitigate risks of programmers implementing programs without approval, changing business information, and changing system functions.

3. Software Change Controls

Given that PRL has recently completed developing and refining its computer-based management information system and that internal company operations such as accounting and billing are supported by in-house developed systems, the company must have adequate system change controls in place.

(1) System Change Control Policy and Procedures

As I've already mentioned, it is my understanding that there is very little control exercised over the Information Services Division by other parties within the company. As such, any change control policies have been developed by the Information Services Division rather than the organization itself. Given the extensive implications that in-house developed systems have on functions such as accounting and billing, it is crucial for the organization to take a more active role in defining change management policies, particularly with regards to the thresholds for approving changes. A change control board, consisting of IT management and cross-section managers, will also be beneficial as it will create more pressure for the development of systems that provide data that can be analyzed using standard management information retrieval tools.

(2) System Change Tracking

Unfortunately, during my review of the activities of the Information Services Division, I did not come across any systems that are in place that adequately document and communicate system changes to management and the rest of the organization. It is crucial for the company to have change management systems in place, for both planned and emergency changes, that document changes, create audit trails, and send an automated notice to management. This will help PRL ensure that all changes are properly documented, tested, and approved and that all key managers are aware of any updates made to the information systems that they are currently using in their functions.

(3) Code Comparison

Given that a complete and detailed audit trail is provided by means of extensive transaction code and related to the batches of original vouchers that are stored on optical disks, it is important for PRL to compare current source code for all internally developed

systems to the backup or yesterday's source code. Changes should then be reconciled with the approval audit trail. This will ensure that the automated audit trail will clearly show the impact of system changes on transaction information. PRL's current system change control policies do not require such reconciliations and therefore do not provide internal and external auditors with the information they need to evaluate the effectiveness of the company's internal controls.

4. Access Controls

It is important for organizations to secure access to computing environments, specific systems, and important functions. Based on my observations, the company must strengthen its access controls in the following areas:

(1) Information Access Controls

First of all, in terms of information access controls, PRL does not have any processes in place that assess the sensitivity of information in order to link this information to specific security tools. As it stands, a substantial amount of sensitive information, including salesmen's commission statements, payroll registers, and customer mortgage statements, are provided to all major departments of PRL without consideration as to whether access to this information should be limited in order to reduce the risk of this information being manipulated or misused. There are also no security standards in place that address privacy concerns associated with the wide distribution of this information. PRL can therefore not address the concern as to whether the information that it distributes has been handled appropriately and with confidentiality. In order to preserve the integrity of its sensitive information, the organization must first define what information and reports each department needs in order to perform their functions. Next, the organization must have a system in place that identifies and tracks all of the information and reports that each recipient in a department receives. This will allow PRL to trace any changes made to this information to a specific department or recipient and will ensure that access to sensitive information is limited to individuals who can specifically be held accountable for the security and use of this information.

Secondly, the company does not have procedures in place to prevent the insertion of "non-essential" data to files. In addition, a user department clerk can add and change data within a file without hard copy documentation. This gives rise to considerable concerns over the authenticity and reliability of information in PRL's data files. In order to remedy such weaknesses, the organization must have a repository of information owners which contains the names and titles of all individuals that make additions or changes to information in data files. The company must also maintain hard copy documentation of all major changes made to data files. Once again, I would also like to stress the importance of having user authentication systems in place such as password controls to ensure that only specified individuals are capable of accessing and changing data files.

(2) Physical Access Controls

Currently, the organization does not have sufficient access controls in place to limit access to important functions. For example, one of the organization's most important functions (the mortgage system) can be accessed from any one of the firm's 300

workstations. This creates an opportunity for any user to access, change, or delete any information in PRL's key function systems.
The organization must have procedures in place to grant and disable access to important systems and information stored in these systems (e.g. user authentication through password controls) and must keep detailed access logs in order to better identify and investigate any unauthorized access. The organization may also want to consider physical access controls such as having only a limited number of workstations that can access important functions. These data centres should be separate from the other workstations and the use of these data centres should be monitored and limited to only certain individuals.

(3) General Access Controls

Aside from the specific access controls mentioned above, there are also a number of general access controls that the organization must have in place. Most notably, because the company uses a wide area network that is accessible from each of the 10 branches in Canada, automated controls such as firewalls, intrusion detection systems, and encryption software must be in place. PRL must also have a system in place that identifies and grants access to representatives of each branch to share information systems and data files. Intrusion prevention and detection as well as privacy are of considerable concern as PRL must have sufficient security standards in place to ensure that any information shared amongst its 10 branches will be used appropriately.

5. Systems Development and Acquisition Controls

I am sure that you are aware that systems development methodology is critical for effectively initiating and approving IT projects, I do however have some concerns about the systems development methodology currently used by PRL:

(1) Senior Management Involvement

A major weakness in the development of information technology systems at PRL is the lack of senior management involvement in the development process. This lack of oversight by senior management and reluctance to become involved in information technology development is a substantial weakness because it leads to a development process void of important senior management feedback.

Improving the systems development process requires the joint efforts of senior management and the manager of the Information Services Division, Billy Chow. This joint effort would create synergy in the development process as Mr. Chow provides an expert development perspective while management may offer a more high level organizational perspective. This suggested control would not only improve the development process but also mitigate the risk of development failure due to having only a single source of input, which is currently only Mr. Chow.

In order to further mitigate the risks of systems development, management should create and enforce a comprehensive process for the development of projects in the information technology division. This process should include criteria that new projects must meet in order to receive approval, and a number of senior management signoffs at

important milestones in the project's life. The process for systems development approval should be carefully designed to balance out two very important aspects: 1) to involve management in the development process and 2) to empower Mr. Chow to continue his highly productive work. This can be achieved through a process which allows Mr. Chow to receive quick approval in order to avoid slowing down his progress in development.

(2) Extent of Documentation

Another weakness in the systems development process is the lack of documentation. Documentation allows other employees and auditors to gain a better understanding of the development process and the results of final products. This mitigates the risk of having a small group of people lead the development of an important project. While producing the documentation may slow down the development process, it is vital to reducing risk and therefore should be done as part of the development process.

6. Disaster Prevention Controls

PRL should take steps to protect its information technology systems against general threats of disaster which any organization faces. General disaster prevention includes taking measures such as installing fire extinguishers in data centres, surveillance equipment monitoring high threat areas, alarm systems, back-up power generators, and adequate cooling systems for machinery. While I have noted some disaster prevention controls implemented by PRL, there are some areas that are lacking:

(1) Adequate Communication

Upon my investigation of the Information Services Division at PRL, I noted a lack of communication between Mr. Chow and the rest of the organization. Due to the prominent role that Mr. Chow plays in the Information Systems Division of the company, any prolonged period of loss of communication with him could lead to serious problems. In order to mitigate this risk, the organization should be capable of functioning normally without him.

While Mr. Chow claims his division staff could continue without him, the facts paint the opposite impression. It appears as though Mr. Chow prefers to work in isolation, independently of team members or senior management and has engineered several of the company's internal systems himself. To reduce this risk, staff in his division should be adequately trained to continue without Mr. Chow. Proper documentation of information systems, testing, and changes should also be made to enable staff to gain insight into any existing information systems.

Other avenues are also available to help mitigate the risk of disaster at PRL such as purchasing an appropriate insurance policy. The company should also create a comprehensive disaster recovery plan to expedite the recovery after a disaster does occur. In the short-term, after a disaster the use of redundant communication lines helps access vital information, while for the long-term additional back-ups should be implemented.

7. Incident and Disaster Recovery Controls

According to Mr. Chow, PRL has been able to maintain strict, high-quality incident and disaster recovery controls through the use of simulated emergency situations. Nonetheless, to ensure that the operations are not disrupted during unforeseen circumstances, the company must establish internal controls in the following areas:

(1) Data Retention and Backup

PRL currently uses an optical disk to store batches of original vouchers for transactions. Such use of physical storage increases the possibility of tape mishandling and should be replaced with an electronic vaulting system. Furthermore, the new system must have an automated backup system that saves data on a regular basis.

(2) Software Backup

The source and object code for ongoing software projects must be backed up on a daily basis or as changes are made.

(3) Data Backup for Batch Systems

The batch system used to process the transactions is critical for producing accurate financial data. Therefore the backup for this system must be updated on a daily basis. For master and transaction files, I have noted that the organization only keeps one version of these files. This indicates that the files do not contain a sufficient amount of data as required by the Canada Revenue Agency and the Internal Revenue Service (i.e. they contain less than 7 years of data). PRL must establish a strict policy to keep at least three versions of such files. This would also support the audit of the current fiscal year's financial statements.

(4) Data Backup for Online Systems

The backup procedure for the online system master file is completed in a different manner than the procedures followed for the backup of a master file for a regular batch system. The file must be updated as transactions occur and a new file must be created on a daily basis to accommodate any important changes. In addition, the organization must decide on how many times the backup must be updated throughout the day.

(5) Incident Response Procedures

Specific incident response procedures must be developed to provide employees with proper guidance on how to handle certain situations. When deciding on the procedures, management must designate an appropriate number of levels (generally less than 5 levels) to ensure that the process is not too bureaucratic or cumbersome.

8. System Operations Controls

It is clear that Mr. Chow maintains a control-free approach to system operations controls dealing with daily operations. Therefore I would specifically like to address controls in the following five important areas in order to achieve sufficient system operations controls:

(1) Procedures to Cover IT Purchases

It is critical for management to maintain a Total Cost of Ownership (TCO) approach in its IT purchase approval procedures where a designated authority approves purchases depending on the value of the transactions. In addition, because PRL purchases a proportion of its software from outside sources, the organization must ensure that the software is compatible with the company's operating system before the purchase.

(2) Procedures to Cover IT Deployment

PRL must develop a policy to ensure that installing new software or hardware is always approved by management and only done by qualified personnel who have expertise in the field. Similarly, certain configuration standards must be decided on and distributed to employees to increase system uniformity.

(3) Network Documentation

The programmers and analysts at PRL do not follow specific documentation procedures even though they are continuously involved in the programming, testing, and maintenance of several information systems. Although this approach allows programmers to interactively work on a program, PRL must have network documentation in place to troubleshoot and effectively implement network changes. Under the current system, analysts only provide assistance on a needs basis, which may not be sufficient when a proper change needs to be implemented. Troubleshooting for TREB and ASP systems are also provided inconsistently and formal documentation should be established to better address customer needs.

(4) Server and Network Configuration

PRL should develop different policies and procedures to guide the server and network configuration for TREB and ASP systems. They must be regularly updated and reviewed to make any necessary changes.

(5) Network Monitoring Procedures

There are three ways that PRL can prevent errors in network monitoring: 1) using equipment that generates the least amount of errors, 2) designing safe circuit configurations, and 3) choosing the appropriate data transmission methodology. In particular, it is important to have data transmission redundancy procedures using methods such as parity checking and cyclical redundancy checking to minimize data loss.

MC Questions How does 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 chief information officer.
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 the correct one-to-one correspondence in number?

a) Library and environment
b) Programmers and testers
c) Source code and object code
d) Master file and transaction file

9. Which of the following library 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 outside consultants occasionally to advise with respect to system development activities
d) Appointing the CIO to the firm's IT steering committee

CHAPTER FOUR

Review Questions

1. What are the different phases of system testing and who are involved?
   Programmers test their own code and this is called unit testing. Peer testing among programmers is called string testing, sometimes involving the testing of code written by different programmers. The entire system or a major subsystem is tested by independent testers and this is called system integration testing. Finally, user representatives test the entire system and this is called user acceptance testing.

2. If an organization hires a firm to develop a system, how does the organization ensure that the system will be maintainable?
   The user organization can include in the contract that the source code and related system documentation like system flowcharts will be given to the user organization upon contract breach by the developer or another form of contract termination. Arrangement can also be made for such documentation to be periodically provided to the user organization during the contract. A third control is to arrange for the source code and supporting documentation to be periodically deposited with an escrow which will allow the user organization to access the documentation upon contract breach by the developer or the developer going out of business, or upon certain other forms of contract termination.

3. What should be included in a request for proposal?
   The RFP should include detailed user requirements. Additional components of the RFP include the evaluation criteria, deadline for submitting bids and a standard.

4. What are the pros and cons of buying a system?
   Pros: Products available without lengthy developmental periods
   Soundly designed and well-tested and thus efficient and reliable
   Reasonable pricing
   Lowers change control risk as the customer is unlikely to have the source code
   - *Cons: General in nature, may not meet all requirements.*
     - *Acquiring firm is dependent on the software vendor for support and maintenance and upgrades*

5. What is a good use of the critical path diagram?
   The purpose is to assess the impact of any delayed tasks on timely completion of the project. Any activity or task on the critical path, if delayed, will delay project completion unless the slack is made up by other activities. There is only one critical path in a project. It is the path of predecessor dependent activities that will take the longest elapsed time.

6. Who should sign off the user requirements?
   Project sponsor, project manager, system design manager, system architecture manager, internal audit, chief information security officer.

7. When should internal controls be first included in a systems development project?
   User requirement phase; this is because users are the best people who know what controls should be in the system.

8. Who should the project manager report to?
   Project sponsor

9. Write a job advertisement for a project manager.
   We are looking for a result oriented IT professional who has experience in managing IT related projects. The person will be responsible for managing IT development projects of varying sizes and working with different business areas of the organization. You will be part of a professional team of project managers in our corporate project management office. Your background should include five years of progressive experience in an IT related field and detailed knowledge of the systems development life cycles for traditional systems and fast paced development. Possession of the Project Management Professional designation will give you an edge. Other skills we look for include:
   - *Team building*
   - *Contract management*
   - *Strong communication*
   - *Consensus building*
   - *Organization*
   - *Financial management*
   - *Project accounting*
   - *Internet networking*

10. Who should be the sponsor of a student records system?
    Registrar

CASE SOLUTION

For this SUD audit of National Land & Water Information Service Project, the audit objectives are identified under three different categories: Project Governance, Business Requirements and Project Management. Procedures were then identified on the basis of the various objectives in order to outline ones that would best achieve the findings described in the audit report.

PROJECT GOVERNANCE

1. Unclear Roles and Responsibilities

OBJECTIVE: "Whether the roles and responsibilities of senior management committees, key project members, users, stakeholders and technical management are clearly defined, documented and performed."

PROCEDURE:

- Verify that roles, responsibilities and authorities are documented in sufficient detail in the Project Governance Chart.
- Verify whether the Project Governance Chart is up-to-date with all recent changes.
- Identify whether there are any inconsistencies between the Project Charter and the observed roles and authorities.
- Identify roles and responsibilities which are in the process of changing, ensure that the changes are constructive and compile evidence, if any, of any confusion these changes may bring regarding authorities.

2. Diverse Representation

OBJECTIVE: "Whether the Project Steering Committee has a diverse membership including the Senior Project Advisory Committee (SPAC), IT and senior management who, together, would provide full coverage of the Project risks, issues, benefits realization, alignment with business objectives and business needs."

PROCEDURE:

- Document who is on the Steering Committee, what professional background they have and their level of seniority.
- Identify any weaknesses in the existing composition of the Steering Committee. Consider unaddressed issues, flow of information and diversity of background experience.

3. Adequate Stakeholder Representation

OBJECTIVE: "Whether the Project Steering Committee has adequate senior representation from NLWIS users."

PROCEDURE:

- Identify stakeholders to the NLWIS project and perform interviews with them to understand their views and expectations for the Steering Committee.
- Assess whether stakeholders are appropriately represented by members on the Steering Committee.

4. Adequate Segregation of Duties

OBJECTIVE: "Whether there are conflicting duties that endanger appropriate segregation of duties."

PROCEDURE:

- Verify that there is appropriate segregation of duties between all Steering Committee members by reviewing all roles and responsibilities and identifying sharing of roles.
- Ensure that the Quality Assurance lead has a direct communication path to the NLWIS Executive Director so that the Project Manager is not perceived as a "filter".

BUSINESS REQUIREMENTS

5. Adequate Prioritization and Validation of Business Requirements

OBJECTIVE: "Whether there is a formal process to assess, document and manage user requirements in system design, construction and process execution."

PROCEDURES:

- Obtain information from management regarding methods for collecting user requirements. Verify that these methods are consistent and effective.
- Ensure that stakeholders have approved architecture and application designs and that there is evidence of their participation and walk-through in the review and approval stages.
- Obtain confirmations from users through interviews that they feel appropriately involved in the process, that communication between them and management is effective and that their concerns are appropriately addressed.
- Trace business requirements through to the design and construction phases through meeting minutes to confirm that that the requirements were delivered by the project.
- Ensure that a thorough and unbiased cost-and-benefit analysis is performed in which stakeholder requirements are prioritized.

PROJECT MANAGEMENT

6. Non-Compliance with Change Management Controls

OBJECTIVE: "To find a mature process for the management of project and system related changes as well as evidence for that the process is followed. A mature process would involve users, development staff and in some cases IS/IT security personnel."

PROCEDURES:

- Identify the roles of the members of the committee responsible for approving the changes
- Confirm that items recorded in the change control log can be traced to the recorded decisions
- Ensure that all key stakeholder groups have the ability to input change requests, by reviewing history of change requests and interviewing parties who are able to input requests, to ensure there is no obstacle preventing them to do so
- Trace a sample of recent changes to the minutes of the Change Control Board meetings, to ensure that no change requests were made without appropriate approval

7. Ineffective Risk Management

OBJECTIVE: "To find a mature risk management process whereby risk mitigation plans are developed, monitored and escalated as required. There should also be sufficient evidence of risks being addressed on a timely and proactive basis"

PROCEDURES:

- Check to see if management is using tools, such as the Risk Matrix, to identify components of high risk, and how they can mitigate them
- Ensure that risk mitigation plans are signed off by a designated person upon completion
- Inquire with management and review risk-related reports generated by the company
- Check for meeting minutes of risk management committees to ensure that managers are considering risk management aspects regarding the project as well as that any questions/issues concerning risks are being address in a timely manner

- Review project planning proposals and ensure that there is detailed documentation concerning the progress of the projects as well as any risks involved

8. Limited Performance Monitoring & Reporting

OBJECTIVE: "To find a mature performance monitoring process that leverages standard industry techniques, such as critical path analysis and earned value reporting, to support decision-making and transparency by enabling timely and fulsome performance reporting. Also, to find evidence of effective and mature performance reporting that supports project monitoring described above as well as address reporting requirements."

*Critical path diagram on page 202: it shows the interdependence and sequence of tasks needed to be performed as part of a project, and their duration, to identify the length of the project and set budgets and deadlines.

**Earned value is a very useful metric used in financial monitoring procedures which measures benefits realization by identifying whether actual expenses incurred are consistent with business plans; in essence, earned value measures the extent of useful time spent on a project

PROCEDURES:

- Verify that an adequate monitoring infrastructure is present for all full-time and part-time project resources.
- Identify the existing performance metrics and confirm that no gaps exist in performance reporting.
- Verify that realized benefits are effectively measured and linked to cost.
- Ensure that a system is in place to provide a complete assessment of project status regarding schedule, budget, benefits and the nature of existing or potential problems. Confirm that the system reports further on the "earned value", incorporating delivery of benefits and outcomes.

9. Insufficient Transition Planning

OBJECTIVE: "To find evidence of an end-state plan for the NLWIS Project in order for the project team to transition NLWIS to the future business owner responsible for ongoing service delivery."

PROCEDURES:

- Accumulate evidence of transition planning, specifically the end-state impact of the NLWIS project. Evaluate whether sufficient estimates and information is provided on how the project will be sustained after completion. (e.g. annual operating costs).
- Ensure that the in-service model for NLWIS is updated regularly, as per changes undertaken throughout its development stages.
- Evaluate whether it is reasonable to conclude that the project will reach a timely completion.
- Identify the team responsible for sustaining the project after completion and ensure that their roles and responsibilities are sufficiently documented.

MC 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 upgradeability and maintainability?

a) Registration of the system
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

1. What is the similarity between PIPEDA and Electronic Commerce Act?
   They both protect consumers and apply to organizations that offer eBusiness.

2. Which risk does eBusiness affect the most?
   eBusiness increases the concern about transaction authorization and information privacy because of the nature of the Internet.

3. What is the consequence if a domain name server is hacked?
   A user may be directed to a hacker site or if the DNS is down, outgoing traffic can come to a halt.

4. What are the audit implications of EDI?
   More reliance on controls, e.g., EDI controls particularly with respect to security. Less substantive testing for inventory because companies can use EDI to achieve better "just in time" inventory.

5. What is the difference between URL, IP address and MAC address and what are the risk implications?
   Every Internet transaction has to include these addresses in order for it to be routable. 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 does not change. 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 forensic investigation.

6. What are the risk implications of RFID?
   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? This concern is understandable as privacy breaches are often reported in the media. 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 less than adequately controlled deployment of RFID.

7. What are the key controls to protect intellectual property?
   Registration
   Access controls
   Contracts with software developers, consultants and employees re intellectual rights.
   Management monitoring of access to and use of intellectual property
   Employee education

8. How do you think the audit of Google differs from that of General Electric?
   More control testing for a company like Google and less substantive testing. This is not to say that control testing is not important for GE. There are more systems in GE so the variety of controls is higher. More real time testing for Google because of the higher fluidity of transaction. No inventory in Google.

9. How does eBusiness affect the five system components of infrastructure, software, people, procedures and information?
   More complicated infrastructure
   More software
   Few people in customer service but more technical developers
   Less in house procedures but more help screens and features for customers
   Higher information risk because of the fluidity and online nature of information.

10. Referring to the general controls discussed in Chapter Three, which types do you think are more affected by eBusiness?
    Access and availability.

CASE SOLUTION

Unauthorized User:

This may be the result from several different scenarios:

 An unauthorized user may access the authorized user's account without the knowledge of the authorized user.

 An unauthorized user may access the authorized user's account and make changes with the authorized user's knowledge however this would be a breach of the usage policy and the transactions of the unauthorized user may not be acknowledged by the authorized user. For example, a husband gives his wife his username and password and the wife submits claims without the husband knowing.

The consequences:

The authorized user may not take responsibility for the transactions processed by the unauthorized user. This may lead to confusion regarding health and dental balances and

investigations will have to take place in order for rectification; investigations may be timely and cause inconvenience to both the insurance company and the client

Preventative Measures

1) **Confirmation:** Any transactions processed must be verified by the client through a faxed confirmation. The online claim is sent to the claims department for processing however before payment for the claim is dispersed, the client must print the claim verification, and sign the confirmation and return it to the insurance company for payment disbursement. The client will have 10 business days to fax the claim verification form back to the insurance company. This process may be timely and inconvenient; therefore we can set a threshold for claims over $500. The insurance company should also have signature cards on file to match the claims verification. This will ensure an unauthorized user cannot process claims and deposit the payment into another account.

2) Set up direct deposit for the claimants. The bank information must correspond to the direct deposit information submitted by the claimant's company. Henceforth, any deposits are deposited directly into the pay account of the claimant submitted by the company. Any changes to the direct deposit account must be submitted by the company and not the claimant.

3) Challenge Response: This allow authentication of the user and ensure access is granted to a human being and not a hacking robotic tool.

Detective Measures

1) Management and Independent Review: We can implement a control system to compare claims year over year to observe whether claims are consistent in terms of type and amount. Also, we can compare similar claims over time to see whether the claims are submitted in reasonable timeframes. For example, dental claims for regular dental cleaning

are generally submitted every 6 months. If there are irregularities, we can confirm the claim with the client before processing.

2) Negative Confirmation: We can send a letter right after payment to the client's home address to verify that they have received the claim. If there are any discrepancies, we can advise the client to contact the claims department immediately. This is a negative confirmation to confirm that the claim was properly processed and payment was made to the authorized client.

2. User Input Error

This risk is related to the authorized user inputting the claims information incorrectly.

Consequences:

The claim may be processed under the wrong category or for an incorrect amount

Preventative Measures

1) We can implement system edits to ensure that appropriate information is inputted into the correct fields.

For example:

a. Payment amounts must be numerical and in a specific format.

b. First Name and Last Name fields must be alphabetical characters

c. We can have a drop down menus for the allowed types of claims (dental, medical, orthodontics, other)

d. Postal codes should be in the correct sequence

2) If claim values are above the benefit dollars we can have a message to prompt the client to enter a lower amount that is allowed.

Detective Measures

1) Boundaries: We should set upper and lower limits for the most common claim values for specific types of claims. If the client inputs higher or lower claim amounts that do not fall within these limits we should have further verification procedures before processing the claim. We can contact the client or the medical professional directly to investigate the details of the claim. This will ensure the claim type is correct and legitimate.

2) For claims over a material amount such as $5000, we should have secondary verification by a claims specialist before payment processing. Since these are large claims we can investigate to ensure there is are no keying input errors. Also, this investigation can further ensure the claims are legitimate, follow the insurance claim criteria, and ensure fraudulent activities are not occurring.

3. Unauthorized Transactions

Employees risk losing the chip based coverage card, employee's personal information may be stolen in the process of accessing website - unauthorized transactions

Preventive

1) eBusiness Encryption - Secure Sockets Layer (SSL) creates an environment where there is a secure area for data which runs between the web browser and the web server; ABC's website must have access to a server that is supporting the SSL application. This requires both parties to have the appropriate technology, SSL is normally present in Microsoft Internet Explorer browser.

2) Password - Employees are encouraged to change their passwords frequently, therefore, even if the employee lose their card, unauthorized users cannot log into their accounts even if they "steal" the cards from the employees

Detective

1) Access Card - employees required to sign a form upon card issuance committing to inform ABC when the card is lost, the access control system online should track all the card usage. Access cards should be coded to indicate the employee that is using the card (confidentiality)

2) Lock - Since dentists and pharmacies insert their coverage card to a card reader on their PCs to submit claims, there should be instructions given to laptop or PC users to lock it to fixtures while unattended, furthermore, ABC should periodically patrol for compliance.

4. Unauthorized Changes to Employee Profile

Employers can enrol their employees via the web site - thus, employers may be able to change employee's profiles or compromise their information

Preventive

1) Access Control List - Different users should have different rights to access the information. Although employers can enrol their employees via the website, the right to make changes to information should only be granted to the employee, although employers still have the right to read the information. Therefore, the system has to be told who to allow to access to what and to what depth through an access control list. The employee should have full access to its information (read, write, delete), but employers should only have the right to read (unless the employee have stopped working for the company, then employer has the right to delete too). This ensures access only based on authorization, to maintain the confidentiality and integrity of information provided to both the employee and the employer.

2) Passwords - Again, employees are encouraged to change their passwords often, so that its employers will not have unauthorized access to their accounts. Furthermore, the employees is encourage to adopt different passwords for different systems, as this will

help decrease the risk of exposing all of one's records in all systems when the password is compromised.

Detective

1) Monitoring and Alerts - To ensure the unauthorized changes are identified in a timelier manner and to minimize the damage that ABC's customers may face, effective monitoring processes must be implemented. First, a log entry must be created for any events that happen on the account. Furthermore, a mechanism should be implemented to notify the employees of these events if there are changes to their accounts (even if the changes were made by them). The mechanisms can be an email alert, or a telephone message.

2) Log-in feature - A security feature that ABC may implement on its web site is to allow employees to see the last few accesses made to their own account. Therefore, if anybody else, such as their employer have been able to log into the employee's account, then the employee is able to acquire this information by verifying the last login activity feature. ABC should provide employee the detail as to when the account was accessed, whether it was using a regular web browser, or from a mobile device, furthermore, the IP address should be identified as well. For employees, seeing information such as the IP address is important because if the employee know that they always use the same computer to access the account, the IP address will be the same, however, if it is a significantly different address that they see, the employee is able to detect that someone else had access their account.

5. Unsecured Channel

Employers can enrol their employees via the website – possible unsecured channel for transferring confidential information

 It is expected that when employers create an account for their employees they would be transferring highly confidential materials such as bank accounts, sin number, address etc. If not handled properly, it is possible to have their accounts breached and identity stolen or hackers may have information altered before reaching ABC

Preventive

1) A representative from ABC Life Insurance can visit their clients on a regular basis to personally collect information from the employers. After giving personal information to the representative from ABC, the employer should require them to sign a document indicating that they have received the documents. In the event of a breach, the people who had access would be held accountable; hence, with action accountability, the people would be less likely to misappropriate use the information

2) If information were to be sent via the website, there should be an encryption of the information. In order to access the locked document, it would require a decryption key. The decryption key would be sent via another channel (e.g. mailed or e-mailed) or at a different point in time

Detective

1) On a regular basis contact ABC to ensure the banking information which they received is identical to those provided by the employer. There should be a materiality level depending on the size of the company.

2) Firewall/ Intrusion Detective and Prevention Standard – which scans the source of the incoming traffic which it uses to determine the likelihood of an intrusion. Of course, this would require the systems to have previously designed protective/ preemptive measures when the system detects an intrusion. For example, if it detects a foreign/ undisclosed IP address that would prompt the system to be aware of the incoming information and to take precaution when dealing with it. As there are chances that it is virus which will steal confidential information from ABC's system.

6. Direct Deposit Information Exposed

Claims submitted online can be paid by direct deposit – there are two problems first, it can be hacked so that these claims are deposited into another person's bank account. Second, the direct deposit information can be exposed to unknown parties.

Preventive

1) After ABC has received a claim submission, they should confirm with the employee before approving the payment with regards to the amount and the bank account

2) ABC should attain WebTrust and/ or SysTrust certification which indicates that they have sufficient controls for online transactions

Detective

1) ABC should provide guidelines on how long the employee should wait before they receive their payment. If it has been an exceeding amount of time then that particular claim/ transaction should be investigated.

2) After the deposit has been made by ABC, the employee has to (within a certain period of time) confirm payment in the correct amount. Then ABC can sample a number of claim of a period of time to identify the instances which the claims was processed incorrectly.

7. Risk of Online Claims Submission by Dentists and Pharmacies

Dentists and pharmacies can submit claims online - giving access to 3rd party and making it inherently risky (privacy concerns since unauthorized transactions more likely)

Preventative

1) Instead of giving access to dentists and pharmacies, they can hire someone or put a current employee in charge of inputting the information for dentists and pharmacies. This gives them less access and give them the ability to control the risks of information getting out to other parties (although may not be cost effective)

2) Add finger print login for the websites (new laptops typically have finger print identification systems – ex. Yahoo enables users to login by finger print)

Detective

1) Review claims submitted by pharmacies and dentists on a daily basis. Ensure that appropriate information and amounts are being inputted, as well as checking for any errors that may have been inputted

2) Send customers a copy of their claims and ask for an affirmative response. Ask them to reply if it is correct or if there are misstatements on the claims

8. No Mitigation of Risk of Unauthorized Transactions

Chips were launched at an accelerated scale - they're not doing themselves a favor and aren't mitigating the risk of unauthorized transactions

Preventative

1) Launch limited chips for the dentists and pharmacies. Limiting the amount of dentists and pharmacies that can use this chip will lead to lower risks of fraud

2) Go through a screening process that will only grant chips to trustworthy dentists and/or pharmacies or only grant chips to long-term dentists and pharmacies associated with ABC Life Insurance

3) Limit all the chips transactions to occur at a certain hour of the day to avoid suspicious chip activity

Detective

1) Call customers and employers randomly, one a week, to verify transactions and to ensure that each transaction exists and/or is accurate

2) Have someone authorize transactions of amounts higher than the materiality level (which should be set by ABC Life Insurance Company)

3) Review claims annually to ensure adequate provision for responsibilities, billing arrangements, security and privacy

MC 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 prospective employer asks for your citizenship.
c) A bank uses an employee's doctor notes to assess whether to approve the employee's loan application.
d) A life insurance company asks about your medical history.
e) A government job application form asking 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 Ontario 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) Ryerson University
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

REVIEW QUESTIONS

1. What is the difference between redundant data check and referential integrity check?

   Redundant data check is a network control that inserts redundant data in each packet which is a derivative of the main data in order for the receiving node to check the integrity of data transmission. The receiving node uses the same algorithm as the sending node to calculate the derivative (redundant data value) and compares the calculated value to the received redundant data. After that, the redundant data is discarded by the receiving node. Referential integrity check is a database control to check that every record in a table has a non-blank value for the foreign key to ensure that the record has integrity. A foreign key is a field in a table that is primary key in another table. For example, each course table in an active firm must have an instructor, so the instructor number in the active course table is a foreign key.

2. What is the difference between batch total and hash total?

A batch total is 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. A hash total is 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.

3. Describe an example of what can go wrong if concurrent update is allowed.

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 at the same time, 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 savings 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.

4. Describe a technique that can be used as a general control and an application control.

   There are many techniques. A common example is a system alert on change. For example, when production source code is changed, the software change management system should send an alert to the system owner. Similarly, when a pay rate is changed, the payroll system should send an alert to the employee's supervisor.

5. A common football tactic is to surround the quarterback of the opposing team. Draw an analogy between this and internal control.

This is called preventive control, some might even equate it to preemptive control. The latter is not a common term in internal controls, it means a strong preventive control.

6. Which risk do edit checks mainly address?

   Completeness and accuracy.

7. Give an example of a weakness in general control that will lead to seeking high assurance on application controls.

A weakness in general control may not render applicable controls unreliable. That depends on the extent and nature of the weakness. However, there will be impact on applicable controls. The least impact is for the auditors to seek higher assurance on certain application controls, i.e.., on the application controls affected. For example, if a couple of software changes for the payroll system were not signed off by the payroll manager before implementation but were signed off afterwards, the weakness is not severe. To mitigate the weakness, the auditors should conduct more testing of the payroll system controls covered by these 2 change requests.

8. What is the drawback of test data?

Test data is a direct way to test controls. There are 2 drawbacks. First, it provides only point-in-time assurance. Secondly, test data put through a live system may corrupt live data.

9. What is the external auditors' justification for skewing internal control testing towards the first half of the year?

External auditors have to conduct control testing before performing substantive audit work because the extent of substantive testing depends on internal control reliability. Therefore, they typically conduct control testing during mid-year. Close to year end, the external auditors will focus their effort on substantive testing. There is little time for control testing close to year end. This is fine. If controls were found to be reliable at mid-year, the external auditors need only to perform a limited update of control testing at year end by relying on software changes controls. If software change controls are reliable, management will know about software changes. So at year end, the external auditors will first roll forward the testing of software change controls to the extent carried out at mid-year. If software change controls are reliable, the external auditors will ask for a list of software changes since mid-year, and assess their significance. For systems with significant changes, the auditors will update control testing to the same extent as that carried out at mid-year. For systems without significant software changes, the auditors will perform only a limited update of control testing, i.e., the extent of control testing at year end is much less than that carried out at mid-year.

10. What are the similarity and difference between batch total, hash total and run-to-run control total?

They all address completeness. A batch total is 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. A hash total is 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. A run-to-run control total is a batch total taken by the system without human intervention. It is used to check the completeness of data transfer from one system module to another. For example, the payroll system of a company like GE might send batches of labour cost to work-in-progress inventory systems without human intervention. When the data is sent, the payroll system can also send a total for each batch which can be used by each inventory system to confirm the completeness of data transfer.

Case Solution

Case Overview

J.P Morgan implemented the Order-to-Pay system is a web based solution that automated the accounts payable process. There are many benefits of this system that allow companies to optimize their working capital, improving operational efficiency and achieve cost savings. The objective of the system is leaning towards companies to automate the exchange of purchase orders (POs), invoices, payments and discounts by integrating buyers and suppliers via a secure network.

Order-to-Pay provides companies with several advanced approach to accounts payable automation that enhance the control over the end-to-end procure-to-pay process. The way the system provides companies benefit in achieving effective automation for payables, streaming the process and lowering costs by the following three procedures:

1) Speeding the conversion away from paper and manual process
2) Reduce the data entry
3) Easier capture of discounting related to payables

This system is put in place to help a buyer corporation connect to a supplier for exchanging electronic purchase orders, invoices and payments.

Electronic Invoicing and Payment

The capabilities of the Oder-to-Pay system allow for electronic invoicing and payment. It allows the elimination of paper-related inefficiencies from the accounts payable process, lost invoices, reduction in data entry errors and lost vendor inquiries. Electronic invoicing and payment capabilities provide buyers and suppliers the reduction in processing costs by up to 50% or more.

The Electronic invoicing and payment system that is part of the Order-to-pay system allow the communication of invoice status to all suppliers given any form from which the invoice was received by the buyer that can be either through the Order-to-pay system, paper invoices, e-File or from EDI-Electronic Data Interchange. For both a supplier and buyer, the system will provide each with the ability to translate all the data into the formats specified to meet each company recording system. For payment processing, the system facilities the elimination of paper check processing and simplifies the payables reconciliation process by channeling invoices and payments. The system optimizes both the invoice receiving and further the payment system. The optimizing of the two systems provides both the buyer and the supplier company the ability to invest their resources into other department as the Order-to-Pay provides a complete package.

The controls that can be implemented for authorization in the electronic invoicing and payment system can provide a secure system. The first can be employing digital signatures to help ensure that only authorized payments are made for the payment system. Another control can also include amount authorization, basically where ever there is a large amount that needs to be paid to a supplier, will require a second digital signature to

verify the payment made. Further this control can also include a management's override system where the large funds need to be verified by superior. For invoices, when the invoices are transferred there should be a specific authorization control for employees that are authorized to transfer the invoices to the buyer or vice-versa. This type of control can include electronic signature attached to each invoice of a particular employee that can be attached through a password, this will ensure an audit trail.

Since the system for invoice includes data entry and processing, therefore controls are required to cover these areas. For input, the controls for accuracy would include check digit control, where the last digit of a buyer code or supplier code, the last digit can validate the correct buyer in the system. The other checks could also limit checks for dollar values and further staff training is the best source of control to increase accuracy with input. Given that when invoices are sent over to the buyers system from the suppliers system any mistakes can lead to incorrect invoices received by the buyer system. The first control can include batch totals, where all the invoices send for example by the supplier can be added up and then then compared to the total of the invoices received by the buyer, will determine whether the system is working accurately. There is also the translation system that is in place and for this specific system; the total of invoices will act as a great control to assess whether the system is working properly. Further parity checks can also be conducted to assess the continuity of the system and all the data is accurately received by the other party.

The controls for completeness are very important to the system. The reason being again is that because it combines both the input for invoices reducing the paper version plus it combines payment system. For such controls like checking mandatory fields are very important to the whole system. One control can be for checking mandatory fields that will be checked or allowed for the user to check once again before the transaction is complete. Another control for completeness can include. Given it is supplier and buyer network; there should be an emphasis on important fields like the Total, or the buyer number. Such fields need to be shown as verification by the user to verify the values. Some invoices or payment can sometimes not be processed properly and that could lead to unreliable transactions, for such controls are also required for completeness. One such control for completeness can include network transmission controls such as parity checks and redundant data checks. The importance is that the right amounts are transmitted for completeness.

Timeliness is a very important issue because if transactions are not processed on time can become a problem later on the system. Timeliness is more of an issue for processing the invoices and payments and a control can include processing schedule to ensure timeliness. Timing is also an issue for the other party the receiver, if that party is not able to check up in real time any transaction can give them wrong decision making perspective. For such, it is important that the transactions be processed on time and available on time to view. A control can also include management review of process logs.

Working Capital Optimization

By automating the receivables and payables of buyers and suppliers, the order-to-pay system lets companies manage and optimize their working capital depending on their needs. They may be in a position of excess cash and thus take advantage of discounts, or decide to conserve cash flow by deferring payment. They are also able to make changes and adjustments to payment terms easily because of the automated system.The following are controls that would be expected for JP Morgan to incorporate into their order-to-pay system, specifically process controls.

To ensure processing is authorized, the system should have the ability to set limits on credit sales and terms per customer. These system checks would prevent unauthorized inputs from being processed by employees to receive kickbacks for extending more credit sales or providing more favorable terms to customers. In addition, changes to discounts and terms should be restricted to access. Only individuals with access permissions should be allowed to make changes and approve them. Who is given these permissions will vary by organization, but it is expected that JP Morgan would implement this functionality.

For accurate processing, automated system checks should be built in to match discount amounts and payment terms to the limits set in the system when preparing an invoice to customers.

To ensure completeness of payables and receivables, periodic reconciliation should be performed between buyer and suppliers' systems of their receivables and payables owed to one another. These amounts should match, and if they do not, discrepancies should be reported to management.

Finally, timeliness of processing should be upheld by incorporating an aging system for payables. Reporting of these amounts in a schedule should also be possible for management to review the payables periodically.

Supplier Management

J.P. Morgan's supplier management system streamlines an organization's entire supply chain into an easy to use computer based system, replacing the traditional manual systems many organizations currently use. Historically organizations have depended on paper or manual based supplier and vendor master updating processes, ultimately leading to a lack of efficiency as well as potential errors. The system acts as a functioning portal and allows for easy management of all transactions across all suppliers for the company. The supplier management system also has capabilities to be easily integrated into an organization's existing enterprise resource systems and thus improves the ability to oversee all suppliers and transactions. The difficulty with adapting this kind of system is of course in developing the appropriate controls in order to mitigate the risks involved with an entirely automated system.

In order to manage the transaction processing effectively for each supplier, the need for authorization controls are vital for the systems success. With a supplier management system, authorization controls often serve the purpose to prevent unapproved changes being implemented on supplier profiles or transactions being processed. One such control is a review by management of unordinary transactions or changes occurring to supplier profiles. This type of control would prevent a change from occurring that is due to an error or potential misstatement. By having management review unusual transactions, authorization risks can be mitigated using this type of approval process. Another control which could be implemented to prevent unauthorized transactions is a confirmation process with each unique supplier. As the management system has the ability to update supplier profiles automatically, ensuring confirmation would be crucial to avoid potential unauthorized changes from occurring. Authorization controls are very important for the supplier management given that orders are being placed based on existing supplier profiles, thus denying unapproved changes is crucial in order to protect the integrity of the system.

In addition to authorization controls, accuracy controls are also needed in order to prevent transactions from being processed incorrectly. In order to ensure accuracy for transaction generated via the system a matching process would be extremely beneficial for the system. The supplier management system is able to manage both supplier profiles as well as transactions being executed through each supplier, thus matching information at each stage of the ordering process is an important control to have in place. Another accuracy control which can be useful is a reasonableness check. During a supplier profile change or order generation from the corresponding ERP system, assessing reasonability can be extremely beneficial in order to avoid outliers and error filled transactions.

Aside from accuracy the supplier management system also should have controls which ensure completeness. An important control for J.P. Morgan to have in place is a report to be generated each period for supplier information which is not updated. Since the system depends on up to date supplier information for the generation of controls, ensuring that updates are complete is crucial in order to maintain the integrity of the management system. Another potential control to mitigate accuracy risks is that of a confirmation being sent out to each supplier to verify both an update to their profile and transactions are being accurately recorded.

Lastly, timeliness is essential to achieve and thus having internal controls to guarantee that the transactions are managed in an according period and in a timely fashion is also crucial. An important internal control to be utilized within the system is that of a periodic survey with suppliers about the timeliness of orders. This control would give a solid outlook on the effectiveness and timeliness of the system and thus would allow for alterations if need be. In order to solidify the systems timeliness another

possible control is a management review of supplier lists and profiles. The timeliness of the system will depend on its ability to process transactions promptly, and thus with management reviewing the lists there will not be any delays in managing inventory.

Benchmarking and Performance Measurement

The purpose of the benchmarking and performance measurement system is for companies to analyze their procure-to-pay process and optimize the process by focusing on key performance indicators (KPIs). The system measures and benchmarks KPIs in areas such as process automation, working capital optimization and supplier management. Furthermore, the system allows companies to measure their performance by setting objectives for a fixed period of time and then assessing these objectives over time. The system's data will also allow companies to isolate problems for which they can then generate solutions and maximize their operational and working capital savings. To ensure that this system is reliable, J.P. Morgan needs to implement several internal controls.

Authorization is a key objective which must be incorporated into this system in order for it to be effective. The system should have a separate password in place, so that only management or those in charge of performance measurement have access. There should also be controls at the individual companies which restrict input of forecast objectives to management or to restricted employees. If employees are responsible for inputting these forecast objectives, then it is necessary to have management authorization and also notification to management before this critical data is processed.

The benchmarking and performance measurement system should also ensure that completeness is present in the transaction cycle. The system should incorporate run to run controls to ensure proper transfer of data from the main business settlement system to this system to ensure completeness. This will verify that the system has received all transactions generated through the settlement system and thereby ensure that all necessary data is present to calculate the KPIs. This control also ensures the accuracy of transactions passed from the settlements system to this system as the totals can be examined and matched. Also, JP Morgan needs to ensure that there are similar controls for the transfer of benchmarked data based on aggregated industry data.

Accuracy is another key objective which must be met in this system since the accurate measurement of key performance indicators (KPI) for process automation, supplier management and working capital as will affect decision making. Run to run controls can be used here as mentioned to ensure accurate transfer of data from the settlement system to this system. Also, JP Morgan should apply reasonableness check and review data formatting periodically to ensure that settlement data is being inputted or transferred to this system accurately. JP Morgan should also ensure that KPIs are calculated correctly by reviewing the formulas in place, and performing sample recalculations periodically to ensure accuracy of KPI calculations. Benchmarked KPIs should also be subject to similar recalculations and reviews of formulas and also to ensure that industry information is aggregated accurately.

Since management is making decisions to improve performance based on these KPIs, it is important for this information to be timely for it to be useful. One control which can ensure that KPIs are timely is automated data capture from the settlement system to this system. For example, if the % of payments made on time is a KPI, then it is important for the system to have data which is timely so that this KPI is calculated correctly. Another control which could reduce this risk is to use a processing schedule (e.g. daily, weekly), based on how often KPI are examined by management. This will greatly reduce the risk of having untimely information or KPIs being generated. Benchmarked data should also be subject to timeliness by having a recurring processing schedule which should ideally be frequent to meet the needs of companies relying on this information for performance improvement.

Total Settlement

J.P. Morgan's Total Settlement is a system that allows electronic payments for businesses to simplify the transactions between suppliers and vendors. The system processes a variety of methods for payment which include cheques, automated clearing house, commercial cards and wire payments. These multiple payment types are combined in a single file through a self-service web portal which provides suppliers with information regarding payment status, remittance details and the maintenance of payment related information.

It is important for this Total Settlement system to have adequate internal controls in order for it to function effectively. Authorization is a key factor to consider in the controls for Total Settlement. It is important for the documentation and data within the Total Settlement system which includes details on sensitive payment information for multiple businesses to be secure. An example of a control is a privacy policy which clearly outlines to customers using the Total Settlement system what information of theirs is being stored and used and the conditions under which that information is shared or used amongst other users of the system. Another important control is for employees to have restricted access to the information in the system. Only employees who are authorized to make changes should have access to these features and must have the proper approval from management before making changes. Encryption and security features such as firewalls will help maintain the security of the system from outside unauthorized threats such as hackers. For the actual use of the system, proper controls must be in place to prevent occurrences of credit limit breaches and ensure senior management approves of any unusual transactions. Since the system utilizes automated payments, controls for customers to approve any automatically generated transactions to prevent payments being made either erroneously or fraudulently.

With the Total Settlement system rely on electronic data to function, controls to ensure the accuracy of the data being used is essential. Checks for data being used in the system are required to prevent occurrences of incorrect information being input into the

system. These checks can include: check digits to verify product numbers, limit checks to ensure compliance with credit limits for specific customers, sign checks to detect incorrectly entered negative amounts and format checking for dates and alphanumeric data. Other controls to ensure the accuracy of data include locking key fields so that they are not accidentally overwritten and standardized report columns to increase comparability. Confirmation of amounts with customers is required along with a system for customers to have the opportunity to report errors for corrective measures to be taken. Matching these amounts with the purchase order, receiving report and invoices before making payments will improve accuracy.

The nature of the Total Settlement system requires multiple data fields to be input for transactions such as placing orders and making payments for orders. To maintain completeness of the data and guarantee that all required information is input correctly, a user friendly interface with controls requiring mandatory fields be filled in correctly before being submitted should be used. This interface, combined with a final confirmation screen where the employee or customer can review the information being submitted, will verify that the information is complete. Other checks to ensure the validity of the information such as bash total and hash total checks will further improve effectiveness when combined with reconciliation from the transactions journals to the subsidiary ledgers.

Timeliness is important since there is no benefit in the advantages a system provides if the information is not readily accessible to users. Controls to maintain the timely and efficient use of the Total Settlement system include a schedule for users outlining requirements such as when data needs to be entered by and deadlines that need to be met. Combined with reminders to users as well as providing incentives for timely completion will improve the system. To monitor the effectiveness, controls based on metrics for timeliness such as the time it takes for a payment to be completed and analysis of throughput times for orders should be reviewed and compared to objectives to see where improvements can be made. Another important control is the consideration of concerns by users through surveys and suggestions regarding the timeliness of the system to recognize areas where there may be issues with timeliness such as receiving late payments.

MQ Questions

1. A user has accidentally deleted an important document and the disk has been written many times. Which of the following will enable recovery of the document?
   A. A hash
   B. Compressed version stored on another disk
   C. Parity check
   D. Cyclical redundancy check

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. Access
   D. Data storage
   E. Output

3. Which risk does database normalization reduce?
A. Concurrent update
B. Obsolete data
C. Data redundancy
D. Data incompleteness
E. Data leakage

4. Canadian Institute of Chartered Accountants says 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 or medium 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 cheques to the cashier's department. The cashier's department compares cheques to deposit slips. With reference to these processes, what control is missing?

A. Bank reconciliation
B. Batch total of the cheques and remittance advices
C. Credit limit check
D. Joint signatures
E. Cheque endorsement

7. Which type of controls is increasingly taking the place of a traditional output control of maintaining a list for report distribution?

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.

9. When an auditor finds a significant control deficiency, s/he should first

A. conduct substantive testing.
B. ask management to sign for risk acceptance.
C. look for compensating controls.
D. report to the audit committee.

10. An auditor comes across a lot of management overrides when testing application controls. S/he should:

A. test the logging and review of such overrides.
B. be pleased that there are so many management controls.
C. not trust the system.
D. recommend that such overrides not be permitted

CHAPTER SEVEN

Review Questions

1. How does the use of computer assisted audit techniques mitigate detection risk?
   Computer assisted audit techniques allow auditors to test more because of the speed and capacity of computers. This reduces detection risk. Also, there are less inconstancy and errors in interpreting and noticing transaction errors because computers don't get tired and are not biased.

2. State an argument that general audit software packages have limited application in control testing.
   Some critics say that because GAS is used to analyze data instead of system functions, there is no direct testing of controls. Auditors can use GAS to look for evidence of control failure, e.g., account balance over credit limit. However, the absence of such evidence doesn't mean the control worked, e.g., it may just be that no customers had gone over the credit limit even though the sales system did not check that. This argument is less forceful if the auditors used a large sample to test controls. GAS typically lets auditors pick large samples and even the entire population. If the auditor picks a very large sample and finds no evidence of control failure, the auditors', especially external auditors' purpose of control reliance is achieved, i.e., the risk of improper transaction is minimized.

3. What risk does Benford analysis mainly address?
   Benford analysis is used to detect suspicious natural numbers like inventory value, expenses and invoice amounts. It mainly addresses fraud.

4. Describe the relationship between GAS and sampling?
   GAS has functions to support sampling and sample evaluation. With the ability to analyze large data files, a GAS can take the sample size calculation one step further to select samples and also summarize findings.

5. Why is embedded audit module often called continuous auditing?
   An embedded audit module inspects all transactions and subjects each transaction to a set of criteria. A common application is sampling. For example, every 10^{th} loan approved may be selected and copied to a separate file for auditors to access remotely. In addition, the module can perform some audit work in real time, e.g., assessing the reasonableness of interest rate. This is why it is often called continuous auditing.

6. In which industries is integrated test facility more applicable?
   ITF is commonly used in financial institutions. It is suitable to organizations that process real time transactions in a multi-store or multi-branch environment. ITF allows auditors to put test transactions through the live system without distorting real data because the auditors use a test branch which the GL doesn't know about.

7. Why is attribute sampling more applicable in auditing than variable sampling is?
   Auditors are concerned about verifying the correctness of management assertions for internal controls and transaction details. Audit tests will reveal whether each assertion is right or wrong. This is why attribute sampling is commonly used. Attribute sampling is used to obtain assurance on whether the stated attributes are right or wrong or what the actual values are. A common application of attribute sampling is political poll. Variable sampling is used to measure continuous values, e.g., the weights of different items to arrive at an estimated average weight. Although auditors are interested in assessing the value of account balances and transactions, attribute sampling can be used by reducing the unit of measure to a dollar, in which case, attribute sampling will be used to validate the correctness of each dollar. By adopting only attribute sampling (which is ideal for control testing, and can also be used for account value testing), auditor sampling is simpler instead of using both attribute sampling and variable sampling.

8. What risks are analyzed by audit scheduling software?
   Inherent and control risks are measured. The higher the risks, the more frequently a unit will be audited.

9. How do IT trends affect computer assisted audit techniques?
   Computing power doubles annually. This makes computer assisted audit techniques increasingly practical because auditors can test larger and larger samples.

10. What is the relationship between confidence level, population size, sample size and precision?
    Confidence level and sample size are directly proportional; i.e., the more confidence we want to derive from a sample, the bigger the sample size has to be. Confidence level and precision are inversely proportional. i.e., the more confidence we want to derive, the less precision we will have to tolerate, given the same sample size. For example, the chance of a curling rock landing in the red circle is lower than it stopping within the bigger blue circumference. Sample size and precision are directly proportional, i.e., the more precise we want the sample result to be, the more sample items we have to choose, i.e., the more observations. In other words, the longer we observe someone, the better we know that person. Because confidence level, precision and sample size are interdependent, changing one will affect the others. For example, by increasing the required confidence, the sample size has to be increased or precision has to be sacrificed, or a combination depending on the extent of adjustment to the sample size and precision. Population size will affect sample size; up to a point, the large the population size, the more sample items have to be selected. Because of the law of large numbers, once population gets beyond a certain point, say, 100,000 items, sample size needs to change little to obtain the same confidence and precision. For example, it doesn't take 10 times as much water to test the saltines of the Pacific Ocean vs the saltiness of the Mediterranean. All of the above relationships can be automated using computer assisted audit techniques.

CASE

1. Completeness
    a. Objective- To ensure that the amount displayed includes 100% of the transaction amount
    b. Test- Vouch the sales invoices to the A/R ledger
    c. Procedures
        i. Import sales order file
        ii. Use GAS to create an aged schedule of invoices
        iii. Perform a query to select a sample of accounts which are above a certain amount to perform test on
2. Accuracy
    a. Objective- To ensure that the orders under $1000 are accurate and actually occurred Test- Examine orders under $1000 for redundancy
    b. Procedures
        i. Import an aged A/R file and do a systematic random selection of a sample of accounts under $1000
        ii. Check customer numbers for redundancy using GAS
3. Authorization
    a. Objective- To ensure that large transaction over a certain limit were authorized by management
    b. Test- Select a sample of account balances which are higher than the individual's credit limit; check for management signatures
    c. Procedures
        i. Import A/R file and client credit approval listings file
        ii. Use GAS to compare tables and export balances which exceed individual credit limit and perform test to check for signatures
4. Valuation
    a. Objective- To ensure that payments from customers are being received on time so that the account balance is valued correctly
    b. Test- Select a sample of account balances from an aged A/R schedule
    c. Procedures
        i. Import the A/R schedule
        ii. Use GAS to prepare an aged schedule
        iii. Identify customer numbers which have balances that do not fit the prescribed payment terms
        iv. Export those balances and follow up with management

5. Existence
    a. Objective- To ensure that the account balances are resultant from real transactions (customers)
    b. Test- Send out positive confirmations to customers
    c. Procedures
        i. Import A/R schedule
        ii. Use GAS to select a random sample of accounts
        iii. Send out positive confirmations to selected customers

Inventory:

1. Obsolescence
    a. Objective- To ensure that inventory is not obsolete
    b. Test- To review the date of last sale
    c. Procedures
        i. Import Inventory file into the General Audit Software program
        ii. Depending on what is considered obsolete (between 3-6 months), extract items that have not been shipped in the last 3-6 months
        iii. Follow up with management on this list and compare with previous periods to see if holding this much quantity on hand is regular for the item
        iv. If not regular, require the write down of this obsolete inventory
2. Existence
    a. Objective- To ensure that the number of inventory items reported is same as that on hand
    b. Test- Compare physical count to online amount reported
    c. Procedures
        i. Import Inventory file into the General Audit Software program
        ii. Use software to generate random sample of recorded inventory items/balances that should be compared to actual physical count
        iii. Extract list of items and conduct physical inventory count
3. Accuracy
    a. Objective- To ensure controls over inventory are working properly
    b. Test- Perform a system edit check to ensure they are working properly (i.e. doesn't accept negative or large numbers)
    c. Procedures
        i. Import Inventory file into the General Audit Software program

   ii. Use system capability to extract items less than 0 or larger than 100,000
   iii. Follow up with management to see why some items are so large (and require system change if any negative items show up)
4. Authorization
   a. Objective- To ensure that controls are in place whish restrict access to inventory to certain people
   b. Test- Check the physical security as well as the access log to determine who made changes and what changes were made to inventory
   c. Procedures
      i. Import Employee and Inventory files into the General Audit Software program
      ii. Link the tables to see which employees have been making numerous changes (and evaluate time stamp to ensure during working hours)
      iii. Extract list of employees and changes made to follow up with management
      iv. Use list to compare to inventory adjustment listing
5. Valuation
   a. Objective- To ensure that inventory is valued using FIFO
   b. Test- Check COGS and compare physical inventory with purchase orders
   c. Procedures
      i. Import Inventory file into the General Audit Software program
      ii. Use software to generate random sample of inventory purchases
      iii. Extract list and compare with inventory (stock on hand) costs that have accumulated for each item in sample
      iv. Compare aging schedule for inventory purchases and sales (COGS)

MC Question

1. Which of the following number values can be tested with the Benford Law?

A. Social insurance number
B. Student number
C. Store marked down sales price
D. Store inventory value for a product
E. Class size

2. How large does a population have to be for there to be negligible impact on the sample size as the population increases?
   A. 10,000
   B. 100,000
   C. 1,000
   D. 1,000,000

3. Which of the following information is useful in assessing inventory obsolescence?

A. Unit cost
B. Price
C. Quantity on hand
D. Economic order quantity
E. Date of last sale

4. Which type of audit procedures does Benford analysis most directly support?
   A. Substantive testing
   B. Control testing
   C. Analytical review
   D. Audit planning

5. Which type of computer assisted audit techniques requires test data?
   A. General audit software package
   B. Statistical analysis software
   C. Embedded audit module
   D. Integrated test facility

6. A small company claims that its sales order system will not process an order if it exceeds the customer's credit limit. Which is the most effective audit tool for external auditors to test this control?

A. Analytical review
B. General audit software package
C. Test data
D. Observation

7. Which CAAT tool is the most popular?
   A. General audit software package
   B. Embedded audit module
   C. Integrated test facility
   D. Statistical analysis software

8. Which GAS function helps an auditor to determine cheques that are not accounted for?
   A. Dump
   B. Gap
   C. Join
   D. Profile

9. A test approach used to validate processing by setting up a fictitious company or branch in an application for testing transaction processing is called
   A. snapshot.
   B. test data.
   C. transaction tagging.
   D. integrated test facility.
   E. embedded audit module.

10. Which of the following computer assisted audit techniques is most useful in statistical sampling?
A. Test data
B. Integrated test facility
C. General audit software package
D. Embedded audit module

CHAPTER EIGHT

REVIEW QUESTIONS

1. What is the relationship between privacy and access control?
   Access controls support privacy.

2. Who should the chief information security officer report to and why?
   The chief information security officer should report to the CIO because information security is part of IT governance. The CIO is accountable for IT governance with the support of the IT steering committee which consists of also senior executives across the organization.

3. Why is email encryption not very commonly used?
Email encryption is not commonly used because the recipient may not have the same encryption software as the sender and also it requires the sender to click an icon so it is not as seamless as eBusiness encryption which is transparent to users.

4. What are the relationships between access controls and other internal controls?
Access controls support other internal controls. For example, access controls support segregation of duties. They also support exception reporting because by restricting access, unauthorized change to exception reports can be prevented.

5. Which technique is used both in a password control and digital signatures and how?
   Hashing is used in both. A password is hashed using an algorithm to store an irreversibly scrambled value of the password to reduce the risk of password browsing. The same hashing algorithm can be used to produce a scrambled value of a message or document which can then be encrypted using the originator's private key to form a digital signature.

6. How is defence in depth achieved?
   This is achieved by installing redundant and complementary controls in increasing depth of the network, e.g., by installing increasingly rigorous firewalls in a network from the perimeter to interior servers. Another example is installing anti-virus software on different layers of email access points, i.e., Internet email, local email server and individual user computers.

7. What is the difference between hashing and encryption?
   Hashing uses an algorithm to irreversibly scramble value for the purpose of proving integrity. Encryption uses an algorithm and encryption keys to encrypt information which has to be decrypted.

8. Where should an intrusion detection system be placed in relation to a firewall and why?

An IDS should be placed behind a firewall. A firewall inspects traffic according to established criteria and either lets in or keeps out traffic. An IDS inspects the let in traffic to identify any anomaly for individual packets and on an aggregate basis. An IDS does not reject traffic. It alerts security administrators of anomalies who will then, in consultation with management, take action to block further traffic of a similar nature by placing a rule on the firewall that sits in front of the IDS.

9. How does encryption affect anti-virus software tools and what should an organization do to address the effect?

Encrypted files cannot be scanned for viruses. This is why it is critical to have anti-virus software installed on user computers to inspect decrypted files.

10. What security risk can materialize if a domain name server is compromised?

A user may be directed to a hacker site or if the domain name server is down, users cannot access the Internet or in some cases, the Intranet.

CASE

Alibaba.com

Controls for Alibaba

SSL encryption to ensure security of transmitted data.
Digital certificate to ensure that customers are accessing the correct site.
IDS and IPS to prevent its servers from hacking.
Anti-virus
Boundary checking of web input to prevent buffer overflow and SQL injection.
Encryption of stored customer billing and identity data to prevent disclosure to authorized parties.
Security policy to set the foundation of network and application security
Patching of its servers to prevent hacking

This is not a full list.

Controls for Customers

The above may apply to customers depending on their sizes. In addition, the following should be implemented:
Browser security setting standard to prevent from accessing hacker sites.
Password standard to enforce strong passwords.
Firewall to prevent hacking
Hard drive and USB encryption to prevent disclosure of sensitive data.
Laptop locks to prevent loss of sensitive data.

A policy to require that all purchases be made through computers connected to the company's network to ensure complete audit trail and that purchases are made by authorized employees.
Spam filtering to prevent phishing
A standard image for operating system configuration to prevent vulnerabilities.

MC Questions

1. Which of the following provides the strongest protection against hackers?
   a. Operating system
   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 (VPN)
   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. Firewall

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

Review Questions

1. What are the purpose and functions of Active Directory?

   Active Directory serves as a central location for network administration and security. It is responsible 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.

2. What are two common ways to prevent users from installing unauthorized software?

   Do not give user local administration right to their computers. Secondly, insert a clause in the policy on acceptable use of IT resources that people are not to install software without management authorization.

3. What is the purpose of the shadow file?

   Password hashes are hidden from users because no one has a need to read them. The authentication server, of course, has access. Unix hides the password hashes by separating the hash from the user account identity 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.

4. What is the purpose of the sandbox?

   A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third-parties, suppliers, untrusted users and untrusted websites. The sandbox typically provides a tightly-controlled set of resources for guest programs to run in, such as scratch space on disk and memory. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.

5. What type of access does a Special user in RACF have?

   The user can override all RACF resource profile constraints, i.e., s/he usually has access to everything.

6. What are the three types of events recorded in the Windows Log?

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 isn't 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 driver. 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.*

7. What is the function of the password salt and how long is the Unix salt?

A salt contains 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. Unix salts all passwords with a salt length of 48 to 128 bits, depending on user organization preferences.

8. What are the security limitations of the IBM Customer Information Control System (CICS) ?

CICS can restrict access from individual workstations. It also provides restriction of access by users but leaves passwords optional. CICS also 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.

9. What OS components does Resource Access Control Facility (RACF) interface with?

RACF is an external add-on security system that operates on the z/OS operating system. It also interfaces with CICS for transaction processing as well as the IBM Time Sharing Option (TSO) for programming and direct file access via technical user intitated command lines.

10. Where is the Windows salt stored?

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.*

CASE

CASE – Employment Insurance Program

The following is a list of audit findings on operating systems controls for a government employment insurance program (EIP). The auditee was the Department of Information Technology (DIT). These findings were extracted from an audit report dated July 2007, downloaded from the web site of the Auditor General of the State of Michigan.

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 to EIP. Our review of privileged access rights disclosed:

a) DIT did not restrict the security administration privilege to only security administrators. *Requires procedure system configuration changes. Needs to revise the RACF user profiles and the Windows access control lists.*

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. *Requires procedure system configuration changes. Needs to revise the RACF user profiles and the Windows access control lists.*

c) DIT did not prohibit all users from having multiple incompatible privileged access rights. *Requires procedure system configuration changes. Needs to revise the RACF user profiles and the Windows access control lists.*

DIT did not properly secure unemployment 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 EIP 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, social security number and wage earnings without DIT or EIP knowledge. *Requires procedure system configuration changes. Needs to revise the RACF user profiles and the Windows access control lists.*

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. *Requires procedure system configuration changes. Needs to revise the RACF user profiles and the Windows access control lists.*

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 EIP's information systems to users. *Requires procedure system configuration changes. Needs to revise the RACF user profiles and the Windows access control lists.*

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. *Requires policy and procedure changes*

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. *Requires policy and procedure changes*

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. *Requires procedure changes.*

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. *Requires procedure changes*

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. *Requires policy and procedure changes.*

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, and the process for using and maintaining security reports. *Requires procedure changes*

4. 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 protection 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 State 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. *Requires procedure changes*

   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. *Requires policy and procedure changes.*

   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 State'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. *Requires procedure changes*

   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. *Requires configuration and procedure changes. Needs to revise the RACF user profiles and the Windows access control lists.*

Required

1. For each finding, assess whether the solution requires system configuration, management review, policy change, procedure change, or a combination. *Answer highlighted above.*

2. For each finding, recommend a solution. For each solution that requires system configuration, state the solution in the z/OS and Windows environments. *Answer highlighted above.*

MC Questions

1. Which operating system is RACF applicable to?
   a. Windows
   b. Unix
   c. z/OS
   d. Mac OS

2. Which function should be carried out by a system administrator?

   a. Configure the operating system
   b. Configure the database management system
   c. Designing SSO
   d. Changing the sandbox

3. Which of the following pairs is related?
   a. SSO and access control list
   e. SSO and two factor authentication
   f. RACF and Mac
   g. 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 a string like rw--x--- in an access control list?
    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 longest encryption key supported by Mac OS?
    a. 128
    b. 256
    c. 64
    d. 512

10. Who would be a frequent user of TSO?
    a. Bank customer
    b. Programmer
    c. RACF administrator
    d. Database administrator

CHAPTER TEN

REVIEW QUESTIONS

1. What is the effect of outsourcing on the role of internal auditors?
   Outsourcing makes the job of internal auditors more difficult because some audit trail and internal controls are now beyond the organization. If the contract provides a right of audit, internal auditors can go to the service organization to perform audit work. If the contract provides an independent control assurance report, there might be less demand for internal auditors.

2. What is the effect of outsourcing on inherent risk, control risk and detection risk?
   Outsourcing increases inherent risk because it may involve a new way of doing business, also because the parties processing transactions and handling information are new. Outsourcing increases control risks because control procedures may change and also the parties carrying out controls are new. Detection risk is also increased because audit trails and evidence are less directly available.

3. What is the role of the service auditor?
   The service auditor is an auditor hired by a service organization to review and test internal controls asserted by the service organization and express an opinion on the controls in accordance CSAE 3416 or SSAE 16.

4. What is a key difference between CSAE 3416 and SSAE 16?
   Canadian Standard for Assurance Engagements 3416 is the CICA standard that governs how an internal control audit of a service organization should be carried out to provide an opinion on internal controls to the service organization, which will then share with the user organizations. The user organizations can then share the report with their external auditors to bridge the control assurance gap caused by outsourcing. Statement of Standards on Assurance Engagement 16 is the AICPA equivalent standard. It is more rigorous than CSAE 3416 in that it requires the audit opinion to cover the comprehensiveness of internal control objectives in relation to the service description, instead of just on the correctness of service description and the adequacy of internal controls to address each stated control objective.

5. What is the difference between a Type 1 report and a Type 2 report?
   A Type 1 report provides point in time assurance whereas a Type 2 report covers a period of at least six months.

6. Who are the audiences of a service organization control assurance report and why?
   A service organization control assurance report provides an opinion on internal controls to the service organization, which will then share with the user organizations. The user organizations can then share the report with their external auditors to bridge the control assurance gap caused by outsourcing.

7. Can the shareholders' auditor of a service organization also be the "service auditor" in the context of CSAE 3416 and SSAE 16? Why or why not?
   Yes. This is because a CSAE 3416 audit is considered audit service to it does not contravene Sarbanes Oxley Act in terms of the limitation on non-audit services.

8. What are the options to the shareholders' auditors of an organization that has outsourced and which one is the most desirable?
   There are 4 options:
   - *Look for compensating controls in the client organization.*
   - *Test the controls in the service organization.*
   - *Obtain an independent control assurance report on the service organization.*
   - *Perform a substantive audit, last resort.*

   The most desirable alternative is the first one as it is the most expedient. It might not be practical if the extent of outsourcing is significant; in which case, testing the controls in the service organization is the most desirable as it gives the auditors direct assurance.

9. Why do you think a Type 2 control assurance report has to disclose the audit tests?
   A Type 2 report provides assurance over a period which forms a reliable basis for the user auditors to rely on controls. The list of audit tests will help the user auditors assess the consistency of audit tests with the user auditor's own methodology.

10. What level of control assurance is provided by a type 2 control assurance report and why?
    High because the opinion covers internal controls over a period. Similarly a financial statement audit opinion would provide high assurance on financial statement reliability.

CASE

Introduction

ABC is a service organization that provides the HR, payroll, and tax functions for over 150,000 "user organizations" (clients such as financial institutions, schools, and small & medium-sized enterprises). The auditors of these user organizations, termed the "user auditors", require assurance over the internal controls in their client's outsourced HR, payroll, and tax processes. Consequently, a "service auditor" is hired to provide a report regarding internal controls at the service organization to the user organizations (not the user auditor, as they are not accountable to them). The review and testing of ABC's controls is guided by Canadian Standards on Assurance Engagements, particularly the

CSAE 3416 standard (equivalent to SSAE 16 in the United States), to obtain assurance on the internal controls on each control objective. The report may be Type 1, giving assurance at one point in time, or Type 2, giving assurance over 6 months or more. In this case, the report written is an SSAE 16 Type 1 report on internal control design. However, the case asks for audit procedures that could have been conducted on the internal controls described from the perspective of a CSAE 3416 Type 2 report on internal control design and operational effectiveness.

1. Employment Manuals

Control: When a new employee is hired, they receive an employee manual that contains company policies including acceptable use and confidentiality. Each employee is required to sign a form that acknowledges that they have received the employee manual.

Control Objective: The objective of this control is to ensure that all employees have signed the form, which acknowledges they received the employee manual. This ensures that every employee has a thorough understanding of company policies including acceptable use and confidentiality. This prevents mismanagement of information and leakage of confidential information.

Procedures: Obtain a list of newly hired employees in the past year, and see if all employees have signed and submitted the form which indicates they have received the employee manual. This list can be vouched to actual copies of the forms.

2. Employee Hiring Procedures

Control: Following a "new hire checklist", the HR Manager obtains a reference and criminal background checks prior to start date.

Control Objective: The control objective here is to ensure that the hiring process for employees are fully completed.

Procedures: Obtain a check list of employee to ensure that HR Manager follows it; match it with all the supporting documentation (reference check, criminal background check, etc.).

Control: Following a termination checklist with assigned tasks to be completed upon the employee's termination. Tasks are assigned to the Human Resource department, the employee's supervisor and IT-related employees, as applicable.

Control Objective: The control objective is to ensure that proper termination procedures are followed and that terminated employees' access to sensitive information are terminated.

Procedure: Obtain the termination checklist for employee and verify that steps have been checked off with appropriate signatures for each task, signifying that they have been completed.

3. Orientation & Training

Control: Monthly meetings are held to discuss issues from the prior month and this ensures that there is on-going job-related training for each employee.

Control Objective: It is to ensure employees in Payroll Processing are correctly using the payroll system.

Procedures: Examine the meeting minutes of the Payroll Processing department and ensure that all issues on the agenda are resolved and all action items are assigned and followed up in the next meeting.

Control: ABC, Inc. holds company-wide meetings on a quarterly basis to communicate company information including new policies.
Control Objective: It is to ensure that company information, such as new policies, are effectively communicated to all the employees
Procedures: Examine the meeting minutes on quarters where new company policies have been implemented. Ensure that the new policies were on the agenda of those meeting minutes and check that employees have acknowledged the meeting minutes to ensure that they agree about what was discussed.

4. Staff Performance
Control: After formal annual performance evaluations are conducted by senior management, and feedback is provided by the employee's direct supervisor, the evaluation is added to each employee's HR folder.
Control Objective: The objective of this control is to ensure that formal annual performance evaluations are conducted by a member of senior management for each employee.
Procedures: Obtain a sample of performance evaluations from the employee folders. Check to see whether the evaluations include feedback as well as an appropriate signature by matching the signature on the evaluations to a name on the list of senior management.

5. User Access Controls
Control: Establish physical controls over the custom developed software located on local workstations. Physical access controls should be monitored and passwords should be changed periodically
Control Objective: The objective of this control is to provide security on the custom developed software and prevent it from being damaged, or tampered by unauthorized individuals.
Procedure: The security can be tested by attempting to access the software through dummy passwords (i.e. trying to input fake passwords). A schedule of how often the password is changed, as well as the character requirements of passwords should be obtained and reviewed to ensure that they are adequate.

Control: Establish controls to ensure that only authorized personnel are granted access to the custom designed software. Furthermore, controls should be established to ensure that access for authorized personnel is reflective of their job responsibilities.

Objective: The objective of this control to ensure the confidentiality, integrity, and availability of company information. Only personnel with the appropriate job responsibilities and authority should have access to the software.
Procedure: Obtain list of authorized personnel with their level of authority in the system (whether they can view, edit, and/or delete documents in the system); review their title and responsibilities to ensure its reasonableness.

Control: Establish controls for adding, changing and deleting user access within the custom designed software.
Control Objective: The objective of this control is to prevent unauthorized individuals from having the ability to tamper with who has access to the software.
Procedure: Test the control by actually trying to add, change, or delete a user.

Control: Establish controls for assigning and monitoring password security for workstations with administrative access to customer designed software. When employees are transferred to other areas of the institution or are terminated, new passwords should be created. Each user should have a unique user ID and password.
Control Objective: The control objective is to ensure that only the employees that currently have authority have access to the software. Employees that have been transferred to terminated should no longer have access.
Procedure: Obtain a list employees who have been transferred or terminated in the last month (or several months) and the dates they were transferred/terminated, and obtain a corresponding schedule of when passwords have been changed to determine if the appropriate procedures have been followed.

7. Change Management
Control: Patches are applied after appropriate approval from an authorized employee is granted and testing has been performed.
Control Objective: It is to ensure that patches are only applied after there is appropriate approval from authorized employee and testing has been performed.
Procedure: Examine approval forms and vouch to list of authorized employees to ensure that approval is only granted by employees on the list. Sample a few change applications to compare the time when the patch is applied to the time when the approval is granted and when testing has been performed. The patch should be applied after approval has been granted and testing has been performed.

Control: Changes to institution parameters are requested by authorized individuals and that a review of completed institution parameter changes is performed.
Control Objectives: It is to ensure that unauthorized individuals cannot change the institution parameters and the review is to ensure that only the necessary changes were made to the parameters.
Procedure: Examine a sample of the change request forms and vouch to the authorized individuals list to ensure that only authorized individuals are submitting change requests. Sample reviews done after the parameter change and vouch to the change request form to ensure that only the requested parameter has been changed and the review was performed correctly.

Control: Support requests can only be sent in my authorized individuals and they must be followed up timely.
Control Objective: The objective is to ensure that support requests are submitted only by authorized individuals and are followed up within the proposed time limit.
Procedure: Examine a sample of support requests and vouch to the list of authorized personnel to ensure that all the requests are only submitted by those with authorization.

Then, examine a sample of support requests and compare the amount of time it took for the request to be followed up to the amount of time that the follow up should have taken.

8. Network Security

Control: Firewalls and other equivalent security devices are implemented as access controls.
Control Objective: The objective of this control is to ensure that network systems that are connected to ACB Inc. are protected from public networks.
Procedure: Obtain a list of firewalls and security devices installed. Obtain a list of instances when the firewall denied network transmissions and unauthorized access to ensure only legitimate communication was allowed to pass.

Control: All changes to institution parameters are requested from authorized individuals and a review of completed changes is performed.
Control Objective: The objective of this control is to ensure that no unauthorized changes are made to institution parameters. The review ensure that only the necessary changes were made.
Procedure: Obtain a sample of change request forms and match the name and signature on the forms to a list of authorized individuals. Sample reviews performed after parameter changes and vouch to the change request form to ensure that only the requested parameter has been changed and the review was performed correctly.

Control: A process to review and install operation system-level patches on workstations running the custom developed payroll processing software is implemented.
Control Objective: The purpose of this control is to ensure that the payroll processing software on all workstations is free from technical bugs and up to date.
Procedure: Obtain reviews indicating the workstations requiring operation system-level patches and vouch to a list of workstations that installed the patch.

9. Disaster Recovery Planning

Control: The applicability of the disaster recovery plan and the results of the annual disaster recovery plan testing are reviewed. A comprehensive business continuity plan is developed to correspond to the disaster recovery plan.
Control Objective: The objective of this control to ensure that the company can continue to operate smoothly without disaster. Specifically, to minimize the potential downtime that could be experienced if a disaster was declared at either ABC Inc. or their own organization.
Procedure: The steps of the disaster recovery plan and business continuity plan should be obtained from management, as well as the results of this year's testing. These documents should be reviewed thoroughly and any weaknesses/failures noted should be discussed with management.

10. Organization & Administrative

Control: A formal organizational chart that establishes proper delegation of authority is used.
Control Objective: The control objective is to provide reasonable assurance that through employees have an adequate understanding of the company structure and organizational chart, and are clear about their responsibilities and level of authority.
Procedure: Obtain the formal organization chart to verify that a delegation of authority exists.

Control: Each employee is assigned responsibilities based on formally defined job descriptions.
Control Objective: The control objective is to ensure that all employees are aware what their responsibilities are and have appropriate knowledge.
Procedure: Obtain a copy of job titles and their responsibilities; vouch it against a formally defined job description.

Control: The Employee Manual is reviewed annually by the CEO for applicable updates.
Control Objective: The control objective here is to see whether the CEO actually reviews the Employee Manual annually and make the appropriate changes.
Procedure: Obtain this year's Employee Manual and check for the CEO's signature as a sign of review and see if changes are made.

Control: Company policies are documented in an employee manual and made available to each employee.
Control Objective: The control objective is to ensure that all employees are aware of the company policies and they can refer back to the manual.
Procedure: Obtain an employee manual to verify that company policies are documented in it.

Control: Employees receive and sign acknowledgement of the Employee Manual at the time.
Control Objective: The control objective is to document the fact that all employees are aware that they received the Employee Manual at the time.
Procedure: Obtain an Employee Manual and vouch for appropriate employee signature.

Control: A formal new hire checklist is used during the hiring process.
Control Objective: The control objective here is to ensure that through recruiting, hiring, evaluation and training process, employees possess the necessary skills and conform to organizational policies and ethics.
Procedure: Obtain hiring checklist and see that it's been checked off to verify that it is used as part of the hiring process.

Control: Annual evaluations are performed for each employee by senior management.

Control Objective: The control objective is to verify that all employees have been properly evaluated and given ongoing feedback.

Procedure: Obtain an annual evaluation for an employee and review it for senior management signature.

Control: Ongoing internal job related training is provided to each employee.
Control Objective: The control objective is to ensure that all employees have the appropriate knowledge to carry out their responsibilities through training.
Procedure: Review the list of internal job related training available to employees, how they are available and obtain the attendance sheet (or any other records) of those trainings.

Control: Companywide meetings are held on a quarterly basis to communicate new information including new or updated policies.
Control Objective: The control objective is to verify that ABC Inc. is communicating new information including new or updated policies to its employees so that they are aware of any changes.
Procedure: Obtain meeting minutes and vouch for the date to verify that those meetings are indeed quarterly. Review the meeting minutes to ensure that announcements are made.

Conclusion

The audit procedures conducted by the service auditor is likely similar to what the user auditor themselves would have done if the HR, payroll, and tax functions had not been outsourced. However, given that the outsourcing of services is becoming more and more prevalent, it is clear that the reports provided by the service auditors to provide assurance over internal controls of outsourced services are essential to user auditors.

MC Questions

1. Which of the following firms can conduct a CSAE 3416 or SSAE 16 assurance engagement?
   A. IBM
   B. McKinsey & Co.
   C. KPMG
   D. Microsoft

2. Which is an option that is always available to the shareholders' auditor of a corporation that has outsourced?
   A. Take a primarily substantive audit approach.
   B. Rely on compensating controls in the client.
   C. Test the internal controls of the service organization.
   D. Rely on an independent internal control assurance report.

3. Which requirement forms a key difference between CSAE 3416 and SSAE 16?
   A. One of these standards does not allow a point-in-time assurance report.
   B. One of these standards requires the service auditor to opine on the adequacy of internal control objectives.
   C. They differ on the requirement for subsequent event disclosure.
   D. They differ on the extent of audit procedures disclosure.

4. From an organization risk perspective, which is the greatest risk factor of outsourcing to an offshore location?
   A. Threat to local economy
   B. Higher cost
   C. Challenge by Canada Revenue Agency or Internal Revenue Service
   D. Contract dispute resolution
   E. Impact of foreign legislation

5. Which option is always available to the management of a service organization if a service auditor cannot rely on a stated internal control?
   A. Replace the internal control
   B. Fix the internal control
   C. Remove the internal control objective
   D. Stop the engagement

6. What level of control assurance can the user auditor derive from a service organization control assurance report?
   A. High
   B. Moderate
   C. Low
   D. Moderate for a period report

7. What is the period of testing for internal controls in a type 1 control assurance report?
A. One day
B. Three months
C. One or more days
D. At least six months

8. Which of the following internal control deficiencies is most correctable by a service organization in an independent control assurance engagement?
A. Weak password
B. Lack of testing of disaster recovery plan
C. Back-up not stored offsite
D. Late management review of staff absence record

9. The disclosure of audit procedures in a type 2 report helps
A. service organization management to assess the comprehensiveness of audit testing.
B. user organizations to assess the comprehensiveness of audit testing.
C. user organization auditors to assess the comprehensiveness of internal control testing.
D. the shareholders' auditors of the service organization to support its financial statement audit opinion.

10. What should the service auditor do if the internal controls pertaining to a control objective are inadequate?
A. Withdraw from the engagement.
B. Qualify the audit opinion.
C. Provide an adverse opinion.
D. Delay the report.

CHAPTER ELEVEN

Review Questions

1. Map the SysTrust principles to the control matrix we discussed in Chapter Six.

	Security	*Integrity*	*Availability*	*Confidentiality*	*Privacy*
Completeness		*x*	*x*		
Authorization	*x*	*x*		*x*	*X*
Accuracy		*X*			
Timeliness			*X*		
Occurrence	*x*	*x*			
Efficiency			*x*		

2. How does SysTrust differ from CSAE 3416 in terms of the comprehensiveness of assurance?

CSAE 3416 coverage depends on the services provided by the service organization, whereas SysTrust requires that security, processing integrity and availability be covered in all cases.

3. What are the management options to avoid a qualified SysTrust audit opinion when a significant control deficiency is found?

Fix the deficiency if the period in which the deficiency is tested to have worked covers a high majority of the reporting period.

Replace the control with another control if the period in which the replacement control is tested to have worked covers a high majority of the reporting period.
Cancel the engagement or turn it into a CSAE 3416 audit or a special review.
Drop the SysTrust principle if the principle affected is confidentiality or privacy.

4. What does the SysTrust audit opinion cover?

It covers the correctness of system description and the adequacy of internal controls to address each SysTrust principle. The comprehensiveness of control criteria is also covered.

5. What parties can benefit from a SysTrust audit report?

Hosting organization management, user organization management, user organization auditors, hosting organization's internal audit department.

6. What kinds of organizations are held to comply with the Payment Card Industry Security Standard?

Any organization that takes credit card transactions electronically.

7. What kinds of organizations are required to provide an annual external validation of compliance with the PCI Security Standard?

Any organization that accepts credit card transactions electronically and processes at least 1 million credit card transactions annually; or any organization that processes at least 20,000 credit card transactions electronically.

8. According to the PCI Security Standard, what kind of access should be monitored?

All access to credit card data.

9. How does the PCI Security Standard affect the financial statement audits of large retail merchants?

They likely will need an annual external validation of compliance. They have to implement more access controls. Access controls are better which make the audit easier.

10. How does the PCI Security Standard affect the profit of large retail merchants?

They likely will need an annual external validation of compliance. They have to implement more access controls. Over time, there will be less credit card fraud and customers will be more inclined to buy over the Internet which should reduce the cost of major retailers.

CASE When an organization hosts an information system a level of assurance on internal controls may be demanded by internal and external users. The Canadian Institute of Chartered Accountants (CICA) has developed a framework and guide for providing assurance over these controls. This type of internal control assurance is called Systrust and this trust standard is defined with using the five trust service principles of security, availability, processing integrity, confidentiality and privacy. The first three principles must be used by the service organization and the remaining two of confidentiality and privacy are optional.

In regards to the Independent Electricity System Operator (IESO) an outline of the five principles surrounding Systrust are described below:

Security

Security refers to the protection of the system from unauthorized access, both logical and physical.[1] Limiting the unauthorized access to IESO's system will prevent abuse and misuse of the system and allow for system protection. Assuming IESO's full statute-based standards include the proper access controls the following policies, communication, procedures, and monitoring need to be defined and outlined.

Policies

IESO's security policies are established and periodically reviewed by authorized individuals. These policies are identified and documented in a written form that are approved by the IT steering committee that ensures both IT and physical access to the

[1] 533

company's forecasting database are limited to certain individuals.
Entity's security policies include:

- Policies to prevent unauthorized access through use of passwords to lock computers and systems as well as assigning access cards with different access levels for employees
- Maintaining a log of access to IESO's systems
- Identifying and mitigating security breaches and use of a firewall for preventive and detective purposes

Communication

- The IESO will need to have a prepared description of the system and make users aware of the access points available
- Personnel responsible for changing security policies surrounding IESO's information system are responsible for updating the policies and communicating any changes
- Breaches to IESO's system will need to be communicated to authorized users

Procedures

- The IESO has proper procedures in place to identify potential threats of disruption to the systems operation as well as an assessment of the risks associated with the identified threats
- Strict access controls are in place to restrict data entry and correction capability to authorized individuals
- A log must be kept for users that access the data entry system
- Data must be backed up every day and stored off-site
- Installation of firewall will prevent unauthorized access from hackers

Monitoring

- Monitoring is essential for IESO as compliance of the system security policies need to be maintained in order to ensure no security breaches have occurred
- Reviewing access levels of employees on a periodic basis to add, modify, or remove employees who no longer need access

Availability

IESO must meet the availability principle in order to ensure that their system is accessible to all the electricity market participants including the generators, transmitters, retailers, industries and businesses, distributors and consumers. IESO matches the offers to supply electricity from generators with the IESO's forecasted demand in order to provide the consumers with the market prices and direct the required amount of electricity. Furthermore, IESO assesses the reliability of the system and the adequacy of existing generators and transmitters to meet growing demand. Therefore, it is important that the information provided by the IESO system is available on a continual basis. The minimum acceptable performance level for system availability is set by the IESO's reliability standards which are established through mutual agreements between IESO and the market participants.

Policies
In order to ensure availability, IESO must define and document its policies for the availability of its system. It is also important to document which personnel is accountable for developing and maintaining IESO's system availability policies. The documented policies and accountability should be reviewed regularly and approved by a designated individual or group. A list of possible IESO system availability policies is available under the security principle policies.

An important system availability policy which is co-ordinated by IESO is the Emergency Preparedness Plan. The Emergency Preparedness Plan describes how market participants will respond to emergencies which may affect the supply or transmission of electricity and how IESO would recover the information for all the market participants. The responsibility for the documentation of the local emergency plan is assigned to each authorized market participant. The compiled Emergency Preparedness Plan should be reviewed by IESO and each authorized market participant should submit a compliance form as part of their annual review process. IESO should also assign the responsibility for documentation of the policies in backing-up data, storing it in an alternate data centre, and recovering the data in case of an emergency. Furthermore, any updates or changes to the emergency plan policies by IESO or by each market participant should be authorized, tested, and documented.

Communication
IESO must communicate its system availability policies to all the authorized users. The IESO should communicate the following information to all its authorized users: an objective description of the system and its boundaries, the availability obligations of IESO and the market participants, accountability for the system availability policies and policy updates, and the process for submitting system availability issues and complaints.

IESO communicates that its purpose is to connect all of its participants, including the generators, transmitters, retailers, distributors, and consumers. The Emergency Preparedness Plan which includes a description of the emergency response procedures, communication procedures, and the processes for restoration and recovery of power and information is effectively communicated to all the authorized market participants. The availability obligation of IESO and the market participants and the accountability for each emergency process in the Emergency Preparedness plan is also communicated to all the authorized users. Finally, updates to the Emergency Preparedness plan and any availability issues is submitted by each market participant to IESO who then reviews and communicates the information to all authorized users.

Procedures
In order to ensure that IESO achieves its documented system availability objectives in accordance with its defined policies, it has procedures in place to identify disruptive threats that would impair system availability commitments and the assessment of the risks associated with the identified threats. First, IESO should have a backup, offsite storage, restoration and disaster recovery consistent with its system availability policies.

IESO should also have procedures to restrict logical and physical access to its system such as firewalls, back up media, servers and other procedures listed under the security principle. IESO should also identify, report, and address system availability issues. IESO should also use encryption and security techniques to protect information

IESO should also have system availability procedures in place for daily back-up of data, storage of data in an alternate data centre, and immediate recovery of data in case of an emergency. The IESO Emergency Preparedness Plan should also have emergency response procedures, health and safety procedures, communication procedures, and the procedures for restoration and recovery of power and information. IESO and the market participants should also be responsible for communicating and training its employees in implementing the procedures under the Emergency Preparedness Plan. It is also essential to test the emergency plan at least annually and also to perform emergency drills to prepare IESO and its market participants in case of an emergency. Furthermore, any updates or changes to the emergency plan procedures by IESO or by each market participant should be authorized, tested, and documented.

Monitoring

IESO should monitor the system and maintain compliance with its system availability policies in order to ensure that the system is accessible to all the market participants at all times. IESO must regularly review its system availability performance and compare it with the system availability policies minimum acceptable levels. It should identify and address potential impairments in its ability to achieve its system availability objectives. Any environmental, regulatory or technological changes should be monitored on an ongoing basis in order to assess its impact to IESO's system availability and that the policies are updated accordingly to adjust for externalities.

The IESO's Emergency Preparedness Plan should be reviewed by IESO in order to ensure that the system availability performance of each authorized market participant meets the minimum acceptable levels under their system availability policies. It should also identify and address potential impairments in each market participant's ability to achieve its system availability objectives. Any environmental, regulatory or technological changes that could affect the system availability of each market participant should be updated accordingly in its Emergency Preparedness Plan.

Processing Integrity

Processing integrity is an integral part of IESO's operations as it should exist if IESO's system performs its integral function free of any impairment. This principle refers to the completeness, validity, accuracy, timeliness, and authorization of IESO's data presented to all users.

General policies

In order for the IESO's system to have processing integrity, the IESO must define and document the policies that it uses. The entity must have established policies that protect all aspects of the system's processing integrity. These policies must be reviewed regularly and the IESO must designate personnel to take responsibility of improving

these policies. Ultimately, the policies should help to guarantee that the forecasts and reports are completed in a timely manner and are free from errors. The policies may include the following:

- Identifying and documenting the security requirements of authorized users will ensure that authorized personnel are establishing, monitoring, and enforcing reliability standards in order to maintain the integrity of transactions
- Preventing unauthorized access, which will make sure that there are no unauthorized changes to the IESO's forecasts, reports, and disaster recovery plan and all transactions are can only be accessed by authorized personnel
- Testing, evaluating, and authorizing system components before implementation is critical to the processing integrity of all of the IESO's operations, as it ensures completeness and accuracy. If the IESO did not have such a policy in place, Ontarians would not be sure that the information, forecasts, and reports prepared by the IESO were correct

General communication

Communication is an integral part of maintaining the processing integrity of the IESO's system. This involves communicating documented policies to the appropriate responsible parties and authorized users. First and foremost, the IESO should have a prepared objective description of the system and its boundaries. This must then be communicated to the authorized users, and must include a description of the services the IESO provides and its sources of information. This has clearly been done, as it is evident that the IESO has communicated that its purpose is to work at the core of the Ontario power system and connect all of its participants, including the generators, transmitters, retailers, distributors, and consumers.

The forecasts that the IESO produces every five minutes are used to show consumers the price fluctuation of electricity according to the supply and demand. The information is gathered from the generators' best offers to provide the required amount of electricity. Additionally, the IESO releases regular publications, including the Ontario Reliability Outlook, each of which has a clearly stated objective. For instance, the IESO produces quarterly publications with the purpose of providing 18-month forecasts of the growth in demand for electricity. However, the IESO needs to communicate the sources of information that is used in these publications.

Furthermore, the IESO must make sure that it communicates its procedures for issue resolution regarding processing integrity, which might affect quality, accuracy, or completeness related to complaints. This includes communicating the processes by which an authorized user can obtain support and inform the IESO of any integrity issues. The obligations of users and the IESO's commitments that related to processing integrity must be communicated to all authorized users. As aforementioned, it is important for the IESO to establish policies regarding the responsibility and accountability of the processing system. It is important to note that the IESO must clearly communicate these policies to the personnel who are charged with the responsibility of implementing them. Moreover,

it is essential that any changes that might affect the processing integrity of the system are promptly communicated to management and any authorized users who may be impacted.

Procedures
IESO's operating procedures related to completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs are put in place to achieve its documented system processing integrity objectives in accordance with its defined policies. IESO has proper procedures in place to identify potential threats of disruption to the systems operations as well as an assessment of the risks associated with these identified threats. There are many specific procedures that IESO carries out in its business:

- IESO must check each consumption input of people's usages for accuracy and completeness. The information publicized and consumption forecasts are not accurate without completed inputs on energy consumption. IESO must also review the consumption forecast to ensure that it is complete, accurate, and done on a timely basis. Since these forecasts are used to collect the best offers from generators, it is important that the figures are accurate. Therefore, the review must be done frequently since consumption forecast is carried out every five minutes throughout the province. Frequent review ensures that errors and irregularities are detected, and corrected in a timely manner
- In situations of power outage, the IESO manages the restoration of power on a timely basis by following the procedures as listed on their disaster recovery plan. The disaster recovery plan is regularly tested and the procedures are taught to its employees to prepare for such disasters
- The quarterly 18 month forecasts of the growth in demand for electricity are only assessed for adequate generation and transmission facilities after it has been reviewed for appropriate authorization
- IESO maintains a log of energy consumption throughout the province for a minimum of 10 years.

Monitoring
IESO's operating procedures need to be continually monitored in order to ensure all information used internally and externally is free of misrepresentation. IESO should monitor the following business operations:

- It is essential that IESO monitor the 5 minute forecast consumption changes throughout the province in order to ensure that IESO maintains compliance with the system processing integrity policies. IESO must monitor any potential impairment in consumption amounts and may result in incorrect offers from generators. Any regulatory or technological changes should be monitored on an ongoing basis in order to ensure that all the information presented by IESO on a real-time basis is complete, valid, accurate, and timely.

- In order to ensure that proper procedures have been implemented and that backup is taken periodically, IESO will need to continually monitor the system. In the case of an emergency, the emergency preparedness plan for the province's electricity system needs to be monitored and updated. This would mean that the emergency plan would allow a smooth cut-over and allow operations to continue with the comfort of having complete, accurate, timely, and valid information. By monitoring the status of the emergency preparedness plan, all transactions conducted post-emergency will allow the processing integrity to function free of unauthorized manipulation.
- IESO wants to provide Ontarians with greater access to information about their power system. Thus being so, a level of processing integrity needs to be maintained and monitored in order to ensure that the information provided to the public is accurate, complete, and valid. Through monitoring the information, IESO will be able to identify any potential differences and adjust the information system to present information free of misstatement.
- IESO has full statute-based authority for establishing, monitoring, and enforcing reliability standards in the province. All companies that make up the power system in Ontario must meet these standards. Therefore an integral part of the trust service principle is to monitor compliance and ensure that all users in the power system are functioning according to statute and are free of misstatement. It is vital that compliance is monitored to ensure that there is no breach of contract and that all statutes are upheld. Moreover, any regulatory changes will need to be monitored and their impact will need to be evaluated to make sure that the information presented maintains its processing integrity and all future information will remain in compliance with statute changes.
- The Ontario Reliability Outlook reports on the progress of interrelated generation, transmission and demand-side projects underway to meet Ontario's reliability requirements. It is therefore imperative that this report the system surrounding this report is monitored to ensure that the reports compiled are presenting complete, accurate, valid, timely, and authorized information. If this information did not have processing integrity, Ontario may not meet it's reliability requirements and therefore face any consequences related to their ineligibility. Any changes in the regulations surrounding IESO's Ontario Reliability Outlook will need to be implemented and monitored to ensure that IESO is complying with the new standards and that the processing of information maintains its integrity.

Confidentiality

Confidentiality refers to the system's ability to protect information designated as confidential which includes the communication and transaction of business amongst management and partners and the exchange of information they require to be maintained on a confidential basis. This information is only available to those who need access to it in order to complete transactions or assist in any questions or concerns of business operations. In the case of IESO it is assumed that the confidentiality principle does not directly apply as it appears as though IESO is transparent in all business dealings in the public eye and that in general confidentiality is maintained amongst those with

authorization. Since there is a lack of case facts to apply the confidentiality principle, a conclusion has been reached that an understanding of confidentiality is applied to business transactions that have yet to make their way into the public scope.

Privacy

The privacy principle focuses on protecting personal information when an organization collects information about its customers, employees, and other individuals. Unlike the other principles in SysTrust, there is no privacy control criteria specified in the Trust Services Standard. Privacy guidelines for SysTrust are set according to the Personal Information Protection and Electronic Documents Act (PIPEDA). The ten PIPEDA principles are accountability, identifying purpose, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance.

In this case, the three main issues regarding privacy are forecast consumption data collection (consumer usage history), collaboration with other stakeholders and information shared to IESO by companies that make up the power system in Ontario.

IESO should implement the following internal controls to ensure that the PIPEDA criteria are met and the three main issues regarding privacy are addressed.

Accountability: IESO should designate a senior employee to be accountable for privacy compliance such as the Chief Information Privacy Officer.

Identifying Purposes: IESO should indicate on forms and websites the purpose of collecting all data and provide procedures to staff members in regards to collecting personal information. It is important to state the purpose when information is collected verbally or in free form of written communication.

Consent: IESO should indicate on forms and websites that consent is requested and required where personal information is collected. The company should also 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.

Limiting use, Disclosure and Retention: IESO should develop a retention schedule for personal information, based on purpose of collection. Also, the company should have policies about what kind of data can be disclosed and retained. On a timely basis, data should be reviewed and any unnecessary data that is not used currently should be removed from the system.

Accuracy: Personal information that IESO collects should be accurate, complete, and up to date. Data should not be copied into different systems because data redundancy can cause inaccurate data. IESO should perform periodic verification of personal information

with employees and customers to ensure up-to-date information is recorded in the system. The company should also have regular backups of personal information in case of any unforeseen circumstances. Data should be protected with passwords or pre-screening questions to ensure that only authorized personnel is able to make changes.

Safeguards: IESO should ensure that proper access controls are in place by using passwords and encryption. Data should be also labelled as "sensitive information" so users can be cautious about using it.

Openness: IESO should disclose to its stakeholders about its privacy policies. Privacy policies implemented should be disclosed on the company website and annual reports.

Individual Access: Individual customers who provided information to IESO should be able to review their information and know where their information is being used.

Challenging Compliance: IESO should respond to challenges from the Privacy Commissioner and information owners, such as consumers or employees. The company should document all complaints and periodically a manager should review all outstanding complaints.

MC Questions

1. Which of the following is an optional SysTrust principle?
   A. Confidentiality
   B. Security
   C. Processing integrity
   D. Availability

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 organization(s)

3. Who is responsible for developing control procedures in a SysTrust audit?
   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 of the following differs the most between SysTrust and CSAE 3416?
   A. Flexibility in control objectives
   B. Level of control assurance
   C. Qualification of auditor
   D. Requirement for system description

6. Which organization is most likely exempted from obtaining external scanning for compliance with the PCI Security Standard?
   A. Apple
   B. Amazon
   C. Boeing
   D. Walmart

7. What kind of access to cardholder data must be monitored by Best Buy?
   A. All
   B. Update
   C. External
   D. Create

8. Which of the following sits on the PCI Security Council?
   A. Large banks
   B. Major credit card issuers
   C. Large online merchants
   D. Federal Reserve Board

9. What is the maximum credit card number data that can be displayed to a customer or a merchant?
   A. First 6 and last 4
   B. First 6
   C. Last 4
   D. First 4 and last 4
   E. First 4 and last 4

10. How is a credit card PIN verified?
   A. Comparing the keyed PIN to the database
   B. Comparing the keyed in value to the hash of the credit card number
   C. Comparing the hash of the keyed in value to the hash in the bank's database
   D. Comparing the hash of the keyed in value to the hash stored in the credit card chip

CHAPTER TWELVE

Review Questions

1. What is the shareholders' auditors' responsibility for computer fraud detection?
   Shareholders' auditors are not responsible for fraud detection. However, in audit planning, they should assess the risk of material fraud based on inherent and control risks and take that into consideration in performing analytical review and control testing. If they come across fraud, they should inform management and assess the materiality in relation to the financial statement opinion and management reliability.

2. What is the internal auditors' responsibility for computer fraud detection?
   Internal auditors are responsible for computer fraud detection, because if they aren't, who are? They should consider the risk of fraud in audit scheduling and planning. Their audit programs should be structured to include fraud detection procedures.

3. What are common computer crimes committed against financial institutions and retailers?
   ID theft and credit card fraud

4. Who do you think the chief ethics officer should report to and why?
   This position should report to the chief executive officer because everyone in the organization should be held to high ethics. Such a reporting relationship will show the entire organization that management cares about ethics. The chief ethics officer should also be the recipient of whistle blowing so a high level of reporting relationship is important to ensure that complaints are dealt with without bias and on a timely basis.

5. What computer crimes can result from identity theft?
   Credit card fraud and hacking.

6. What internal controls can organizations implement to prevent system alteration?
   Web site refresh from a backed up version, firewall, intrusion prevention system and patching.

Solutions

7. What are some system controls that can prevent or detect disbursement fraud?
   Watermarking cheques, access control list, cheque limit, system checking for duplicate invoices, system matching invoice to receipted purchase orders.

8. What technology do you think the police and securities commissions use to detect insider trading?
   Benford analysis, regression and other statistical analysis, Encase.

9. How can a bank use analytical review to detect fictitious loans?
   Ratio calculation for each branch and compare to averages for
   Interest revenue / non-interest revenue
   Interest revenue / interest expense
   Non-interest revenue / non-interest expense

10. What is the relationship between Encase and Blancco?
    Encase can be used to image hard disks and recover erased files. Blancco is used to wipe data on a disk so it is not recoverable. Wiping a disk three times using Blancco will render the data completely unrecoverable, even with Encase.

CASE

Question 1:What else could Carlson have done to keep his personal information from Deloitte when the laptop was returned?

Carlson, the defendant argued that he had destroyed the old hard drive because it had personal data on it such as tax returns and account information. As an alternative to physically shattering the hard drive and subsequently replacing it with a new blank one, the defendant could have used basic access controls to prevent unauthorized viewing of personal information. He could have encrypted the personal files on his computer. Encryption could have prevented unauthorized viewing of his personal information by using an algorithm to transform plain text into a coded equivalent. Alternatively, he could have placed passwords on sensitive files to authenticate any users.

The information could be transferred to an external storage device such as a USB memory stick or an external hard drive, however, if the information was originally saved on the hard drive, there are forensic software and procedures which could likely recover the files allowing for unauthorized access.

Prior to returning the laptop, Carlson could have also used disk sanitization or disk wiping software such as Blancco to permanently delete any sensitive files from his hard drive. Charges were made against Carlson because he destroys the hard drive without authorization. There may also be procedures within the firm to dispose of highly sensitive information if he were to consult IT or a relevant authority. Although prior to destruction using their methods, it is likely that Deloitte would first request access to the information to be deleted.

Preventative measures could have been taken to avoid saving any personal information on the hard drive in the first place. Rather than misusing his work laptop by using it to

process and store personal information, he could have used personal equipment or could have simply stored information on a personal hard drive or USB.

Question 2: ***How do you think Carlson communicated with the other employee whom he was alleged to have solicited to leave Deloitte?***

It is likely that Carlson was communicating with the other employee through email. Given that they are connected through Deloitte, it is likely that they were communicating using the internal company email server since this server would give you access to a common address book with all Deloitte employees. A web based email could have also been used, but it is less likely unless they had previously interacted and exchanged personal emails. They could have also been using an internal instant messaging platform to carry on conversations. The other alternative for communication would have been for the employees to use video conferencing. The official case published by the United States District Court of Northern Illinois indicated that Carlson received an email from the other employee with his private email in the subject line, suggesting that there would be additional communication between the two through personal email.

Question 3:***What are some steps you think Deloitte might have used to find evidence of Carlson's loyalty breach or improper system activities?***

Steps that Deloitte might have used to find evidence of Carlson's loyalty breach or improper system activities:

1. Deloitte must have first assessed the situation and understood what type of incident was to be investigated. Deloitte found that it was more than just a coincidence that another high-ranking employee left for the same company as Lyle Carlson (defendant) and that the defendant had erased personal data at the same time. Deloitte assessed the situation to be one in which the defendant

began soliciting another employee to leave before the defendant left, and that defendant allegedly destroyed the data to cover his tracks. First assessing the situation allowed Deloitte to know exactly what type of evidence satisfied their claim. If a situation is not first analyzed, then wrong or weak types of evidence will be gathered and an unclear claim will be rejected in court.

2. After the situation had been assessed, procedures must have been carried out to "freeze" the audit trail. This must have required, for example, sending a request to Deloitte's Internet Service Provider (ISP) to provide Deloitte with internet activity of the defendant just prior to him leaving. It could have also involved copying emails, imaging hard disks, identifying remote storages and imaging the relevant disks and RAM.

3. Physical evidence could also have been examined, such as the extent to which the hard drive had been damaged and whether it was repairable or not. Regardless, the fact remains that Carlson had destroyed the hard drive, which is a strong indication that he had something to hide.

4. Deloitte must have also reviewed system logs to get a general idea of the type of activity the defendant took part in just prior to the defendant leaving. This would have allowed them to make a conclusion on the level of inappropriateness of the defendant's actions.

5. Deloitte could have possibly used special forensic investigation software like Encase to recover erased data. If the evidence of loyalty breach is held on Carlson's email, other specialized software like Discovery Accelerator can be used to search email.

6. Deloitte may have also reviewed Carlson's employment agreement to make sure that there was a clear clause in the agreement forbidding Carlson from soliciting other employees during and after his employment at Deloitte. The presence of such a clause would give Deloitte a solid case against Carlson.

7. Deloitte must have documented all sequence of events, all interviews, time spent by each investigator and the work performed by each investigator. This investigation files must have been safeguarded with encryption and physical measures. Also, it must have been backed up to avoid the possibility of loss.

Solutions

MC 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?
   a. Pull the plug on the computer.
   b. Perform an orderly shutdown on 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 hard disk has been thoroughly wiped by a fraudster using Blancco?
   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

Solutions

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 auditor 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 a forensic auditor 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