

CHAPTER ONE

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. Shareholder value
- 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. The current trouble in European economy has caused the U. S. dollar to fluctuate. What of the following do you think is affected the most?
- A. Cloud computing
 - B. Offshore outsourcing
 - C. Merger
 - D. Cyber warfare
10. In what aspect does the Patriot Act affect Canadian companies?
- A. Outsourcing
 - B. Compliance with the Investor Confidence Rules
 - C. Intellectual property
 - D. Competitiveness

CHAPTER TWO

1. Which database feature increases risk?
 - a) Maintaining data independence.
 - b) Reducing data redundancy.
 - c) **Increases accessibility.**
 - d) Expedites transaction processing.
 - e) Data dictionary

2. Which risk is most affected by social networking sites?
 - a) Reliability
 - 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. 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

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. In 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. 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 6

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 7

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 8

1.	Which of the following provides the strong protection against hackers? <ul style="list-style-type: none"> 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? <ul style="list-style-type: none"> 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? <ul style="list-style-type: none"> a. Security standard b. Security procedure c. Security configuration d. Security training
4.	Which of the following technologies would conflict with encryption the most? <ul style="list-style-type: none"> 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? <ul style="list-style-type: none"> 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 9

1.	<p>Which operating system is RACF applicable to?</p> <ul style="list-style-type: none"> a. Windows b. Unix c. z/OS d. Mac OS
2.	<p>Which function should be carried out by a system administrator?</p> <ul style="list-style-type: none"> a. Configure the operating system b. Configure the database management system c. Designing SSO d. Changing the sandbox
3.	<p>Which of the following pairs is related?</p> <ul style="list-style-type: none"> a. SSO and access control list e. SSO and two factor authentication f. RACF and Mac g. Salt and access control list
4.	<p>Which of the following is run in a sandbox?</p> <ul style="list-style-type: none"> a. Active X b. RACF c. .NET components d. SSO
5.	<p>Which operating system uses CICS?</p> <ul style="list-style-type: none"> a. z/OS b. Windows c. Mac OS d. Unix
6.	<p>Which operating system uses a string like rw--x--- in an access control list?</p> <ul style="list-style-type: none"> a. z/OS b. Windows c. Mac OS d. Unix
7.	<p>When Internet zone is the safest?</p> <ul style="list-style-type: none"> a. Restricted b. Trust c. Internet d. Intranet

8.	<p>Which cookie will still work even with the highest Internet Explorer privacy setting?</p> <ul style="list-style-type: none"> a. Existing persistent b. All persistent c. Existing session d. Session cookies from trusted sites
9.	<p>What is the longest encryption key supported by Mac OS?</p> <ul style="list-style-type: none"> a. 128 b. 256 c. 64 d. 512
10.	<p>Who would be a frequent user of TSO?</p> <ul style="list-style-type: none"> a. Bank customer b. Programmer c. RACF administrator d. Database administrator

CHAPTER 10

MULTIPLE CHOICE QUESTION

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 11

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 scope
 - B. Level of control assurance
 - C. Qualification of auditor
 - D. Requirement for system description

6. Which organization is most likely required to obtain external scanning for compliance with the PCI Security Standard?
 - A. Bank of Montreal
 - B. Amazon
 - C. General Motors
 - D. Office of the Privacy Commissioner

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

8. Who make up the PCI Security Council?
 - A. Large banks
 - B. Major credit card issuers
 - C. Large online merchants
 - D. Bank of Canada

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 12

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

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 suspects to evidence
 - b. Connecting evidence to traces
 - c. Linking suspects to contacts
 - d. Linking contacts to crimes

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

