++T
his demo file contains 25 sample multiple-choice questions taken from the Volume 2 (Practice) of the CISA Examination Textbooks, third edition, published by SRV Professional Publications. Copyright 2001 by S. Rao Valabhaneni.
++

Chapter 1: The Information Systems Audit Process

1. What should the audit strategy be?
a. It should be knowledge-based
b. It should be cycle-based
c. It should be request-based
d. It should be risk-based

Subject Area: IS audit function-Risk assessment. Author 1.1.

Choice (d) is the correct answer. Audits should be planned and conducted according to the risk level; that is, high-risk auditable areas should be reviewed first, followed by medium-risk areas, which are followed by low-risk areas. The medium- and low-risk auditable areas should be reviewed only when audit resources are available. The other three choices do not consider risk explicitly.

9. Which one of the following items includes the other three items?
a. Inherent risk
b. Control risk
c. Audit risk
d. Detection risk

Subject Area: Auditing standards-AICPA. Author 1.9.

Choice (c) is the correct answer. Audit risk is the risk that the auditor may unknowingly fail to appropriately modify his opinion on financial statements that are materially misstated. It is the product of other three risks: it is equal to inherent risk multiplied by control risk, which is multiplied by detection risk. Audit risk is an all-inclusive term here.

Inherent risk is the susceptibility of a management assertion to a material misstatement, assuming that there are no related internal control structure policies or procedures. Detection risk is the risk that the auditor will not detect a material misstatement present in a management assertion. Control risk is the risk that a material misstatement in a management assertion will not be prevented or detected on a timely basis by the entity's internal control structure policies or procedures.

28. According to the COSO report, an effective internal control system requires an ultimate:
a. User
b. Sponsor
c. Owner
d. Customer

Subject Area: Internal control framework-COSO. Author 1.28.

Choice (c) is the correct answer. An effective control system requires an ultimate owner. The only truly effective owner of the control system is the chief executive officer (CEO). The CEO is the only person who can establish the right tone at the top of the organization and who has the power to ensure that all parts of the enterprise effectively communicate and coexist. The ownership responsibility cannot be delegated to an accountant or an auditor.

36. COBIT is the model for which of the following?
a. IT planning
b. IT governance
c. IT standards
d. IT infrastructure

Subject Area: Internal control framework-COBIT. Author 1.36.

Choice (b) is the correct answer. COBIT has been developed as a generally applicable and accepted standard for good IT security and control practices. COBIT is the breakthrough IT governance tool that helps management understanding and manage the risks associated with IT.

Chapter 2: Management, Planning, and Organization of Information Systems

5. The IT function should **not** be used or viewed solely to:
a. Make money
b. Expand the business
c. Save money
d. Increase revenues

Subject Area: IS—Strategic planning. Author 2.5.

Choice (c) is the correct answer. Savings should not be the only criteria for investment in IT projects. The IT investment should facilitate an increase in sales (revenues), expand new markets, introduce new products, and increase income. Current savings should be sacrificed for long-term growth potential.

8. The IT direction must be aligned with which of the following?
a. Cost drivers

b. Business drivers
c. Technology drivers
d. Decision drivers

Subject Area: IS—Strategic planning. Author 2.8.

Choice (b) is the correct answer. The IT direction should be aligned with business drivers, which make the entire organization move forward. All other drivers are subsets of business drivers.

18. Which of the following establishes the boundaries for IT direction?
a. Cost strategy
b. Business strategy
c. Staffing strategy
d. Computing strategy

Subject Area: IS—Strategic planning. Author 2.18.

Choice (b) is the correct answer. Business strategy should drive IT strategy, not the other way around. All the other strategies mentioned are a subset of business strategy.

Chapter 3: Technical Infrastructure and Operational Practices

4. Preventive controls against private branch exchange (PBX) or voice mail system attacks do **not** include which of the following?
a. Disconnecting maintenance lines when not used
b. Enforcing strict rules on password usage
c. Installing physical switches on telephone lines
d. Implementing training and awareness programs

Subject Area: PBX controls. Author 3.4.

Choice (c) is the correct answer. It is important to examine the configuration of the PBX system and correct identified deficiencies. In addition, it is necessary to disconnect maintenance lines when they are not being used for maintenance purposes, to enforce strict rules on passwords used in voice mail systems, and to implement training and awareness programs. Installing physical switches on telephone lines can prevent open microphone listening, but this is expensive and causes the system to lose function.

6. All of the following are controls against network service attacks **except**:
a. Using a floppy disk prior to decompression
b. Removing the network service
c. Concealing the network service
d. Creating traps for network services

Subject Area: Network controls. Author 3.6.

Choice (a) is the correct answer. Traps provide tracing benefits. One can conceal the services by including them within other services so that additional authentication checking is required. It is good to remove network services when not needed. Choice (a) is not an appropriate control in this case.

7. Which of the following tools is **most** useful in detecting security intrusions?
a. Data mining tools
b. Data optimization tools
c. Data reorganization tools
d. Data access tools

Subject Area: Data mining. Author 3.7.

Choice (a) is the correct answer. Data mining is a set of automated tools that convert the data in the data warehouse some useful information. It selects and reports information deemed significant from a data warehouse or database. Data mining techniques can also be used for intrusion detection, fraud detection, and auditing the databases. One may apply data mining tools to detect abnormal patterns in data, which can provide clues to fraud. Data optimization tools improve database performance. Data reorganization tools help relocate the data to facilitate faster access. Data access tools help in reaching the desired data.

103. Which of the following design objectives is **most** important for a local area network?
a. Security
b. Availability
c. Throughput
d. Responsiveness

Subject Area: IS network and telecommunications infrastructure—LAN availability. Author 3.103.

Choice (b) is the correct answer. Availability is the ratio of the total time a functional unit is capable of being used during a given interval to the length of the interval. It is the time during which a functional unit can be used. What good is security, throughput, and response time if the system is shut down, that is, not available? Therefore, system availability is the most important objective for a LAN or any other network.

Chapter 4: Protection of Information Assets

47. Accountability is important to implementing security policies. Which of the following is **least** effective in exacting accountability from system users?

a. Auditing requirements
b. Passwords
c. Identification controls
d. Authentication controls

Subject Area: Security goals. Author 4.47.

Choice (b) is the correct answer. Accountability means holding individual users responsible for their actions. Due to several problems with passwords they are considered to be the least effective in exacting accountability. These problems include easy-to-guess-passwords, easy-to-spoof users for passwords, easy-to-steal passwords, and easy-to-share passwords. The most effective controls for exacting accountability include a policy, authorization scheme, identification and authentication controls (choices (c) and (d)), access controls, audit trails, and auditing (choice (a)).

49. Which of the following provide both integrity and confidentiality services for data and messages?

a. Digital signatures
b. Encryption
c. Cryptographic checksums
d. Granular access control

Subject Area: Security services and mechanisms. Author 4.49.

Choice (b) is the correct answer. An encryption security mechanism provides security services such as integrity, confidentiality, and authentication. The data and message integrity service helps to protect data and software on workstations, file servers, and other LAN components from unauthorized modification, which can be intentional or accidental. This service can be provided by the use of cryptographic checksums (choice c) and very granular access control and privilege mechanisms (choice (d)). The more granular the access control or privilege mechanism, the less likely an unauthorized or accidental modification can occur.

The data and message integrity service also helps to ensure that a message is not altered, deleted, or added to in any manner during transmission. A message authentication code (MAC), a type of cryptographic checksum (choice c), can protect against both accidental and intentional, but unauthorized, data modification. The use of digital signatures, (choice a) can also be used to detect the modification of data or messages. It uses either public key or private key cryptography. A digital signature provides two distinct services: nonrepudiation and message integrity. The MAC can also be used to provide a digital signature capability. Nonrepudiation helps ensure that the parties or entities in a communication cannot deny having participated in all or part of the communication.

66. Rivest, Shamir, Adleman (RSA) algorithm differs from digital signature standard (DSS) in:

a. Digital signature
b. Authentication
c. Encryption
d. Data integrity

Subject Area: Cryptographic techniques. Author 4.66.

Choice (c) is the correct answer. Both RSA and DSS provide digital signature, authentication, and data integrity capabilities. RSA provides encryption; DSS does not. The digital signature algorithm (DSA) is specified in the DSS. The DSS contains the DSA in order to create signatures as well as the secure hash algorithm (SHA) to provide data integrity. SHA is used in electronic-mail and electronic funds transfer applications.

73. Intrusion detection refers to the process of identifying attempts to penetrate a computer system and gain unauthorized access. Which of the following would assist in intrusion detection?
a. Audit trails
b. Access control lists
c. Security clearances
d. Host-based authentication

Subject Area: Intrusion detection. Author 4.73.

Choice (a) is the correct answer. If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Although normally thought of as a real-time effort, intrusions can be detected by examining audit-records as they are created in real time, or after the fact.

Access control lists (choice b) refer to a register of users who have been given permission to use a particular system resource and the types of access they are permitted to have. Security clearances (choice c) are associated with a subject (e.g., person, program) to access an object (e.g., files, libraries, directories, devices). Host-based authentication (choice d) grants access based on the identity of the host originating the request, not the user making the request. Choices (b), (c), and (d) have no facilities to record access activity and thus cannot assist in intrusion detection.

18. The **best** approach to maintaining a contingency plan in order to recover from computer–related disasters would be to use a:
a. Top–down approach
b. Bottom-up approach
c. Combination of top–down and bottom-up approaches
d. Consultant-directed approach

Subject Area: Contingency planning process–Planning approach. Author 5.18.

Choice (c) is the correct answer. The key word is "maintain." Knowledge obtained from testing the plan is useful in refining the plan (bottom-up approach). The changes from management and business conditions and their impact should be considered (top-down approach) when updating the plan. Therefore, a combination of top-down and bottom-up approaches is very useful to maintain a disaster recovery and contingency plan.

24. What is the inherent limitation of a disaster recovery planning exercise?
a. Inability to include all types of disasters
b. Assembling disaster management and recovery teams
c. Developing early warning monitors that will trigger alerts and responses
d. Conducting periodic drills

Subject Area: Risk analysis and evaluation–Assessment. Author 5.24.

Choice (a) is the correct answer. Since there are many types of disasters that can occur, it is not practical to consider all such disasters. Doing so would be cost-prohibitive. Hence, disaster recovery planning exercises should focus on the types of disasters that occur frequently. One approach is to perform risk analysis to determine annual loss expectancy, which is calculated from the frequency of occurrence of a possible loss multiplied by the expected dollar loss per occurrence.

41. The **most** costly disaster recovery alternative is:
a. Mutual backup site agreements
b. Hot-site backup
c. Cold-site backup
d. Off–site archival storage of data

Subject Area: Alternative computer hardware and software requirements–Disaster recovery plans. ICCP XII-4.

Choice (b) is the correct answer. Hot-site backup is most costly, due to the fact that a hot-site is fully equipped and ready to operate. In a hot-site backup, fully equipped commercial computer facilities are used in case of a disaster.

Choice (a) is incorrect because a mutual backup site agreement is least costly. However, mutual agreements are not reliable and may not prove workable when needed. Choice (c) is incorrect because cold-site backup is not as expensive as hot-site backup. However, it is more expensive than a mutual backup site agreement. Choice (d) is incorrect because off-site archival storage of data is not as expensive as hot-site backup. An off–site storage place could be owned by the same organization wanting to process the data.

Chapter 6: Business Application System Development, Acquisition, Implementation, and Maintenance

1. In which of the following system development approaches are systems analysis, design, and testing activities repeated during the life cycle?
a. Prototype
b. Iterative
c. Pilot
d. Grand design

Subject Area: Application system development and acquisition practices-Methodologies. Author 6.1.

Choice (b) is the correct answer. Iterative approach uses a trial-and-error method where analysis, design, and testing activities are repeated to increase user satisfaction with the system design. Choice (a) is incorrect because prototyping is used to define system requirements, and the prototype is repeated until the requirements are fully defined. The scope of the iterative approach, choice (b), goes beyond the scope of the prototype approach. Choice (c) is incorrect because a pilot approach implements a system at one place prior to implementing it in other places. Choice (d) is incorrect because the scope of a grand design is bigger and more complex and does not use the iterative approach.

4. In project implementations, the management tool that is **most** commonly used is called a:
a. Flowchart
b. Process chart
c. Gantt chart
d. Data chart

Subject Area: Application system development and acquisition practices-Project management tools. Author 6.4.

Choice (c) is the correct answer. The Gantt chart is a bar chart used as a project scheduling technique. The structure of the chart shows output plotted against units of time. It gives a quick picture of a project's progress by the status of actual time lines and projected time lines. The other charts do not provide means to track a project during project implementation.

5. The **major** problem in information systems departments is:
a. Inadequate management of system development projects

b. Ineffective control of resources
c. Project cost overruns
d. Project schedule delays

Subject Area: Application system development and acquisition practices. Author 6.5.

Choice (a) is the correct answer. Ineffective information systems departments often result in massive cost overruns, long schedule delays, and systems that do not perform as intended and do not improve an organization's ability to fulfill its mission. The most common category of problems is the inadequate management of the information systems development life cycle. Other problem areas include the inability to ensure the security and integrity of information systems; information systems that do not work together; systems that contain inaccurate, unreliable, or incomplete data; and ineffective oversight and control of information systems resources.

Chapter 7: Business Process Evaluation and Risk Management

1. The **major** purpose of continuous improvement is to:
a. Increase the productivity of employees
b. Document policies and procedures
c. Draw a flowchart of the processes
d. Increase the productivity of systems

Subject Area: Business process re-engineering and improvement. Author 7.1.

Choice (a) is the correct answer. Continuous improvement focuses more on how to improve an existing process or service. The purpose is to increase the productivity of employees, because it is the people who can improve a process or service. The things mentioned in the other choices are minor and secondary.

2. The **major** purpose of change management implementation is to:
a. Allocate resources to implement the change
b. Address people's concerns about the change
c. Develop tools to implement the change
d. Facilitate change agents in the organization

Subject Area: Business process change management. Author 7.2.

Choice (a) is the correct answer. Once management has decided to change a process or service, the next step is to allocate resources to implement the change, regardless of its difficulty in implementation. The other factors are secondary, because without resources no change can be performed. Addressing people's concerns about the change is cultural and a long-term effort. Tools are a part of resources. Change agents were already identified prior to the change implementation.

11. Business process re-engineering (BPR) changes are constrained by:
a. Taking small improvement steps

b. Existing organizational structure
c. Current thinking
d. Current culture of the organization

Subject Area: BPR strategy. Author 7.11.

Choice (a) is the correct answer. BPR changes are not constrained by the existing structure, current thinking, or culture of the organization. Long-standing and ingrained ways of doing things may be radically changed. The changes often include organizational, structural, and procedural changes geared toward achieving multiple results such as improving service delivery, lowering costs, increasing quality, eliminating redundancy, speeding up processes, and others. BPR cannot be carried out in small and cautious steps.

12. Which of the following quality tools or programs uses fear as a key driver of change?
a. Deming
b. Re-engineering
c. ISO 9000
d. Malcom Baldrige criteria

Subject Area: BPR strategy. Author 7.12.

Choice (b) is the correct answer. Re-engineering injects more fear into employees than any other tool or program, because of its far reaching–effects. Deming abhorred the use of fear whereas reengineering proponents use fear to change the status quo. ISO 9000 is less threatening than using the Malcom Baldrige criteria. ISO 9000 is easy and doable and promotes quality systems consistency.