CISA Self-Assessment

The CISA certification was developed to assess an individual's information system assurance experience specific to information security situations. Earning the CISA designation distinguishes you as a qualified information systems assurance and control professional with experience and knowledge assessing information security policies, procedures and controls implemented by an enterprise.

ISACA has prepared the CISA self-assessment to help CISA exam candidates assess their knowledge of the CISA job practice areas and determine in which areas they may have strengths and weaknesses. This self-assessment contains 50 sample items covering the appropriate proportion of subject matter to match the CISA exam blueprint. The items are not actual CISA exam items, but are items developed by subject matter experts in compliance with the CISA item writing guidelines and are meant to provide the exam taker with a sample of what the type of questions that might appear on the exam. Note that this self-assessment is not a substitute for the actual exam, nor does the result of the self-assessment test guarantee or indicate future individual success. For additional exam detail coverage, review each area's task and knowledge statements.

This 50 question self-assessment is one of many tools that you can use to help prepare for the CISA exam.

Enter your name below so it displays on the quiz results page:

Name:

1. A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

- A. IS auditor
- B. Database administrator
- C. Project manager
- D. Data owner

2. An organization's IT director has approved the installation of a wireless local area network (WLAN) access point in a conference room for a team of consultants to access the Internet with their laptop computers. The BEST control to protect the corporate servers from unauthorized access is to ensure that:

- A. encryption is enabled on the access point.
- B. the conference room network is on a separate virtual local area network (VLAN).
- antivirus signatures and patch levels are current on the consultants' laptops.
- D. default user IDs are disabled and strong passwords are set on the corporate servers.

3. An IS auditor discovers that devices connected to the network have not been included in a network diagram that had been used to develop the scope of the audit. The chief information officer (CIO) explains that the diagram is being updated and awaiting final approval. The IS auditor should FIRST:

- A. expand the scope of the IS audit to include the devices that are not on the network diagram.
- B. evaluate the impact of the undocumented devices on the audit scope.
- C. note a control deficiency because the network diagram has not been approved.
- D. plan follow-up audits of the undocumented devices.

4. In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

- A. Approve and document the change the next business day.
- B. Limit developer access to production to a specific time frame.

C. Obtain secondary approval before releasing to production.

D. Disable the compiler option in the production machine.

5. While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

A. recommend the use of disk mirroring.

B. review the adequacy of offsite storage.

C. review the capacity management process.

D. recommend the use of a compression algorithm.

6. During a compliance audit of a small bank, the IS auditor notes that both the IT and accounting functions are being performed by the same user of the financial system. Which of the following reviews conducted by the user's supervisor would represent the BEST compensating control?

A. Audit trails that show the date and time of the transaction.

B. A daily report with the total numbers and dollar amounts of each transaction.

C. User account administration.

D. Computer log files that show individual transactions.

7. From a control perspective, the PRIMARY objective of classifying information assets is to:

A. establish guidelines for the level of access controls that should be assigned.

B. ensure access controls are assigned to all information assets.

C. assist management and auditors in risk assessment.

D. identify which assets need to be insured against losses.

8. To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

A. control self-assessments (CSAs).

B. a business impact analysis (BIA).

C. an IT balanced scorecard (BSC).

D. business process reengineering (BPR).

9. When conducting an IT security risk assessment, the IS auditor asked the IT security officer to participate in a risk identification workshop with users and business unit representatives. What is the MOST important recommendation that the IS auditor should make to obtain successful results and avoid future conflicts?

A. Ensure that the IT security risk assessment has a clearly defined scope.

B. Require the IT security officer to approve each risk rating during the workshop.

C. Suggest that the IT security officer accept the business unit risk and rating.

D. Select only commonly accepted risk with the highest submitted rating.

10. Which of the following BEST describes the objective of an IS auditor discussing the audit findings with the auditee?

A. Communicate results of the audit to the auditee.

B. Develop time lines for the implementation of suggested recommendations.

C. Confirm the findings, and propose a course of corrective action.

D. Identify compensating controls to the identified risk.

11. When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining whether IS:

A. has all the personnel and equipment it needs.

B. plans are consistent with management strategy.

C. uses its equipment and personnel efficiently and effectively.

D. has sufficient excess capacity to respond to changing directions.

12. Which of the following system and data conversion strategies provides the GREATEST redundancy?

- A. Direct cutover
- B. Pilot study
- C. Phased approach
- D. Parallel run

13. Which of the following antispam filtering techniques would BEST prevent a valid, variable-length email message containing a heavily-weighted spam keyword from being labeled as spam?

- A. Heuristic (rule-based)
- B. Signature-based
- C. Pattern matching
- D. Bayesian (statistical)

14. The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- A. understand the business process.
- B. comply with auditing standards.
- C. identify control weakness.
- D. plan substantive testing.

15. An IS auditor discovers that the chief information officer (CIO) of an organization is using a wireless broadband modem utilizing global system for mobile communications (GSM) technology. This modem is being used to connect the CIO's laptop to the corporate virtual private network (VPN) when the CIO travels outside of the office. The IS auditor should:

- A. do nothing because the inherent security features of GSM technology are appropriate.
- B. recommend that the CIO stop using the laptop computer until encryption is enabled.
- C. ensure that media access control (MAC) address filtering is enabled on the network so unauthorized wireless users cannot connect.
- D. suggest that two-factor authentication be used over the wireless link to prevent unauthorized communications.

16. Which of the following is the BEST way for an IS auditor to determine the effectiveness of a security awareness and training program?

- A. Review the security training program.
- B. Ask the security administrator.
- C. Interview a sample of employees.
- D. Review the security reminders to employees.

17. After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- A. Project management and progress reporting is combined in a project management office which is driven by external consultants.
- B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.
- C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy systems.
- D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

18. An IS auditor discovers that some hard drives disposed of by an enterprise were not sanitized in a manner that would reasonably ensure the data could not be recovered. In addition, the enterprise does not have a written policy on data disposal. The IS auditor should FIRST:

- A. draft an audit finding, and discuss it with the auditor in charge.
- B. determine the sensitivity of the information on the hard drives.

- C. discuss with the IT manager the best practice in data disposal.
- D. develop an appropriate data disposal policy for the enterprise.

19. During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

- A. review access control configuration.
- B. evaluate interface testing.
- C. review detailed design documentation.
- D. evaluate system testing.

20. An IS auditor is testing employee access to a large financial system, and the IS auditor selected a sample from the current employee list provided by the auditee. Which of the following evidence is the MOST reliable to support the testing?

- A. A spreadsheet provided by the system administrator.
- B. Human resources (HR) access documents signed by employees' managers.
- C. A list of accounts with access levels generated by the system.
- D. Observations performed onsite in the presence of a system administrator.

21. An IS auditor should recommend the use of library control software to provide reasonable assurance that:

- A. program changes have been authorized.
- B. only thoroughly tested programs are released.
- C. modified programs are automatically moved to production.
- D. source and executable code integrity is maintained.

22. By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

- A. reliable products are guaranteed.
- B. programmers' efficiency is improved.
- C. security requirements are designed.
- D. predictable software processes are followed.

23. Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- A. Financial impact per security incident.
- B. Number of security vulnerabilities that were patched.
- C. Percentage of business applications that are being protected.
- D. Number of successful penetration tests.

24. To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- A. the IT infrastructure.
- B. organizational policies, standards and procedures.
- C. legal and regulatory requirements.
- D. adherence to organizational policies, standards and procedures.

25. An IS auditor is reviewing risk and controls of a bank wire transfer system. To ensure that the bank's financial risk is properly addressed, the IS auditor will most likely review which of the following?

- A. Privileged access to the wire transfer system
- B. Wire transfer procedures
- C. Fraud monitoring controls
- D. Employee background checks

26. Which of the following is the GREATEST risk to the effectiveness of application system controls?

- A. Removal of manual processing steps
- B. Inadequate procedure manuals
- C. Collusion between employees
- D. Unresolved regulatory compliance issues

27. Which of the following is the MOST effective control for restricting access to unauthorized Internet sites in an organization?

- A. Routing outbound Internet traffic through a content-filtering proxy server.
- B. Routing inbound Internet traffic through a reverse proxy server.
- C. Implementing a firewall with appropriate access rules.
- D. Deploying client software utilities that block inappropriate content .

28. If a database is restored using before-image dumps, where should the process begin following an interruption?

- A. Before the last transaction.
- B. After the last transaction.
- C. As the first transaction after the latest checkpoint.
- D. As the last transaction before the latest checkpoint.

29. Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
- B. not include the finding in the final report, because management resolved the item.
- C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
- D. include the finding in the closing meeting for discussion purposes only.

30. An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- A. User acceptance testing (UAT) occur for all reports before release into production.
- B. Organizational data governance practices be put in place.
- C. Standard software tools be used for report development.
- D. Management sign-off on requirements for new reports.

31. Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- A. meets or exceeds industry security standards.
- B. agrees to be subject to external security reviews.
- C. has a good market reputation for service and experience.
- D. complies with security policies of the organization.

32. At the completion of a system development project, a postproject review should include which of the following?

- A. Assessing risks that may lead to downtime after the production release.
- B. Identifying lessons learned that may be applicable to future projects.
- C. Verifying the controls in the delivered system are working.
- D. Ensuring that test data are deleted.

33. To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

- A. examine the change control system records and trace them forward to object code files.

B. review access control permissions operating within the production program libraries.

C. examine object code to find instances of changes and trace them back to change control records.

D. review change approved designations established within the change control system.

34. Which of the following is an implementation risk within the process of decision support systems (DSSs)?

A. Management control

B. Semistructured dimensions

C. Inability to specify purpose and usage patterns

D. Changes in decision processes

35. Which of the following is the BEST way to satisfy a two-factor user authentication?

A. A smart card requiring the user's personal identification number (PIN).

B. User ID along with password.

C. Iris scanning plus fingerprint scanning.

D. A magnetic card requiring the user's PIN.

36. During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:

A. the level of information security required when business recovery procedures are invoked.

B. information security roles and responsibilities in the crisis management structure.

C. information security resource requirements.

D. change management procedures for information security that could affect business continuity arrangements.

37. Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

A. Install the vendor's security fix for the vulnerability.

B. Block the protocol traffic in the perimeter firewall.

C. Block the protocol traffic between internal network segments.

D. Stop the service until an appropriate security fix is installed.

38. An IS auditor should use statistical sampling and not judgmental (nonstatistical) sampling, when:

A. the probability of error must be objectively quantified.

B. the auditor wishes to avoid sampling risk.

C. generalized audit software is unavailable.

D. the tolerable error rate cannot be determined.

39. During the system testing phase of an application development project the IS auditor should review the:

A. conceptual design specifications.

B. vendor contract.

C. error reports.

D. program change requests.

40. After reviewing its business processes, a large organization is deploying a new web application based on a Voice-over IP (VoIP) technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control

B. Role-based access control (RBAC)

C. Access control lists

D. Network/service access control

41. To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) in order to determine:

- A. the business processes that generate the most financial value for the organization and, therefore, must be recovered first.
- B. the priorities and order for recovery to ensure alignment with the organization's business strategy.
- (•) C. the business processes that must be recovered following a disaster to ensure the organization's survival.
- D. the priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

42. An audit charter should:

- A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.
- B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
- C. document the audit procedures designed to achieve the planned audit objectives.
- (•) D. outline the overall authority, scope and responsibilities of the audit function.

43. The PRIMARY purpose of an IT forensic audit is:

- A. to participate in investigations related to corporate fraud.
- (•) B. the systematic collection and analysis of evidence after a system irregularity.
- C. to assess the correctness of an organization’s financial statements.
- D. to preserve evidence of criminal activity.

44. The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- (•) A. improve internal control procedures.
- B. harden the network to industry good practices.
- C. highlight the importance of incident response management to management.
- D. improve employee awareness of the incident response process.

45. When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

- A. Hard disks are overwritten several times at the sector level but are not reformatted before leaving the organization.
- (•) B. All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
- C. Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
- D. The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

46. Which of the following is a characteristic of timebox management?

- A. Not suitable for prototyping or rapid application development (RAD)
- B. Eliminates the need for a quality process
- (•) C. Prevents cost overruns and delivery delays
- D. Separates system and user acceptance testing

47. A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after six months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- (•) A. what amount of progress against schedule has been achieved.
- B. if the project budget can be reduced.
- C. if the project could be brought in ahead of schedule.
- D. if the budget savings can be applied to increase the project scope.

48. Which control is the BEST way to ensure that the data in a file have not been changed during transmission?

- A. Reasonableness check
- B. Parity bits
- C. Hash values
- D. Check digits

49. An IS auditor reviewing a new outsourcing contract with a service provider would be MOST concerned if which of the following was missing?:

- A. A clause providing a “right to audit” service provider .
- B. A clause defining penalty payments for poor performance.
- C. Predefined service level report templates.
- D. A clause regarding supplier limitation of liability.

50. The GREATEST advantage of using web services for the exchange of information between two systems is:

- A. secure communications.
- B. improved performance.
- C. efficient interfacing.
- D. enhanced documentation.

Get Score Reset