Chapter 1

The Audit Process

THIS CHAPTER COVERS CISA DOMAIN 1, "INFORMATION SYSTEMS AUDITING PROCESS," AND INCLUDES QUESTIONS FROM THE FOLLOWING TOPICS:

- Audit management
- ISACA auditing standards and guidelines
- Audit and risk analysis
- Internal controls
- Performing an audit
- Control self-assessments
- Audit recommendations

The topics in this chapter represent 18% of the CISA examination.

This topic is fully covered in the companion guide, "CISA Certified Information Systems Auditor Study Guide," in Chapter 2.

Questions

You can find the answers to the questions in Appendix A.

1. The IT Assurance Framework consists of all of the following except:
   - **A.** ISACA Code of Professional Ethics
   - **B.** IS audit and assurance standards
   - **C.** ISACA Audit Job Practice
   - **D.** IS audit and assurance guidelines

2. An auditor is examining an IT organization's change control process. The auditor has determined that Change Advisory Board (CAB) meetings take place on Tuesdays and Fridays, where planned changes are discussed and approved. The CAB does not discuss emergency changes that are not approved in advance. What opinion should the auditor reach concerning emergency changes?
   - **A.** The CAB should not be discussing changes made in the past.
   - **B.** The CAB should be discussing recent emergency changes.
   - **C.** Personnel should not be making emergency changes without CAB permission.
   - **D.** Change control is concerned only with planned changes, not emergency changes.

3. A conspicuous video surveillance system would be characterized as what type(s) of control?
   - **A.** Detective and deterrent
   - **B.** Detective only
   - **C.** Deterrent only
   - **D.** Preventive and deterrent

4. Michael is developing an audit plan for an organization's data center operations. Which of the following will help Michael determine which controls require potentially more scrutiny than others?
   - **A.** Security incident log
   - **B.** Last year's data center audit results
   - **C.** Risk assessment of the data center
   - **D.** Data center performance metrics

5. An organization processes payroll and expense reports for thousands of corporate customers in an SAAS-based environment. Those customers want assurance that the organization's processes are effective. What kind of audit should the organization undertake?
   - **A.** Compliance audit
   - **B.** Operational audit
   - **C.** Service provider audit
   - **D.** IS audit

6. An audit project has been taking far too long, and management is beginning to ask questions about its schedule and completion. This audit may be lacking:
   - **A.** Effective project management
   - **B.** Cooperation from individual auditees
   - **C.** Enough skilled auditors
   - **D.** Clearly stated scope and objectives

7. An auditor is auditing the user account request and fulfillment process. The event population consists of hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions. This type of sampling is known as:
   - **A.** Judgmental sampling
   - **B.** Random sampling
   - **C.** Stratified sampling
   - **D.** Statistical sampling

8. An auditor is auditing an organization's user account request and fulfillment process. What is the first type of evidence collection the auditor will likely want to examine?
   - **A.** Observation
   - **B.** Document review
   - **C.** Walkthrough
   - **D.** Corroborative inquiry

9. A lead auditor is building an audit plan for a client's financial accounting system. The plan calls for periodic testing of a large number of transactions throughout the audit project. What is the best approach for accomplishing this?
   - **A.** Reperform randomly selected transactions.
   - **B.** Periodically submit test transactions to the audit client.
   - **C.** Develop one or more CAATs.
   - **D.** Request a list of all transactions to analyze.

10. A lead auditor is building an audit plan for a client's financial transaction processing system. The audit will take approximately three months. Which of the following is the best approach for reporting audit exceptions to the audit client?
    - **A.** Report the exceptions to the audit committee.
    - **B.** List the exceptions in the final audit report.
    - **C.** Include the exceptions in a weekly status report.
    - **D.** Advise the client of exceptions as they are discovered and confirmed.

11. Which of the following is true about the ISACA Audit Standards and Audit Guidelines?

- **A.** ISACA Audit Standards are mandatory.
- **B.** ISACA Audit Standards are optional.
- **C.** ISACA Audit Guidelines are mandatory.
- **D.** ISACA Audit Standards are only mandatory for SOX audits.

12. An auditor is auditing an organization's identity and access management program. The auditor has found that automated workflows are used to receive and track access requests and approvals. However, the auditor has identified a number of exceptions where subjects were granted access without the necessary requests and approvals. What remedy should the auditor recommend?

- **A.** Monthly review of access approvers
- **B.** Annual review of access approvers
- **C.** Annual user access reviews
- **D.** Monthly user access reviews

13. Why are preventive controls preferred over detective controls?

- **A.** Preventive controls are easier to justify and implement than detective controls.
- **B.** Preventive controls are less expensive to implement than detective controls.
- **C.** Preventive controls stop unwanted events from occurring, whereas detective controls only record them.
- **D.** Detective controls stop unwanted events from occurring, whereas preventive controls only record them.

14. For the purposes of audit planning, can an auditor rely on the audit client's risk assessment?

- **A.** Yes, in all cases.
- **B.** Yes, if the risk assessment was performed by a qualified external entity.
- **C.** No. The auditor must perform a risk assessment themselves.
- **D.** No. The auditor does not require a risk assessment to develop an audit plan.

15. An organization processes payroll and expense reports in an SAAS-based environment for thousands of corporate customers. Those customers want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?

- **A.** AUP
- **B.** PA DSS
- **C.** PCI DSS
- **D.** SSAE18

16. An auditor is auditing an organization's system-hardening policy within its vulnerability management process. The auditor has examined the organization's system-hardening standards and wants to examine the configuration of some of the production servers. What is the best method for the auditor to obtain evidence?

- **A.** Capture screenshots from servers selected by the systems engineer during a walkthrough.
- **B.** Request screenshots from servers selected by the systems engineer.
- **C.** Request screenshots of randomly selected servers from the systems engineer.
- **D.** Capture screenshots from randomly selected servers during a walkthrough with the systems engineer.

17. An auditor is auditing the user account request and fulfillment process. The event population consists of hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions, as well as some of the transactions for privileged access requests. This type of sampling is known as:

- **A.** Judgmental sampling
- **B.** Random sampling
- **C.** Stratified sampling
- **D.** Statistical sampling

18. An auditor is auditing an organization's user account request and fulfillment process. The auditor has requested that the control owner describe the process to the auditor. What type of auditing is taking place?

- **A.** Observation
- **B.** Document review
- **C.** Walkthrough
- **D.** Corroborative inquiry

19. An external audit firm is performing an audit of a customer's financial accounting processes and IT systems. While examining a data storage system's user access permissions, the staff auditor discovered the presence of illegal content. What should the staff auditor do next?

- **A.** Notify law enforcement.
- **B.** Inform their supervisor.
- **C.** Notify the auditee.
- **D.** Notify the auditee's audit committee.

20. A QSA auditor in an audit firm has completed a PCI DSS audit of a client and found the client noncompliant with one or more PCI DSS controls. Management in the audit firm has asked the QSA auditor to sign off the audit as compliant, arguing that the client's level of compliance has improved from prior years. What should the QSA auditor do?

A. Refuse to sign the audit report as compliant.

B. Sign the audit report as compliant, under duress.

C. Sign the audit report as compliant.

D. Notify the audit client of the matter.

21. An organization wants to drive accountability for the performance of security controls to their respective control owners. Which activity is the best to undertake to accomplish this objective?

A. Direct control owners to sign a document of accountability.

B. Have the internal audit department audit the controls.

C. Have an external audit firm audit the controls.

D. Undergo control self-assessments (CSAs).

22. An auditor is evaluating a control related to a key card mechanism protecting a data center from unauthorized visitors. The auditor has determined that the key card control is ineffective because visitors often "piggyback" their way into the data center. What detective control should be implemented to compensate for this control deficiency?

A. A video surveillance system with 90-day content retention that records all entrances into and exits from the data center

B. A visitor's log inside the data center that all visitors would be required to sign

C. A man trap

D. A policy requiring all visitors to be escorted

23. A US-based organization processes payroll and expense reports in an SAAS-based environment for thousands of corporate customers. Customers outside the US want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?

A. ISO/IEC 27001

B. SOC2

C. ISAE3402

D. SSAE18

24. A large merchant organization has commissioned a QSA (PCI) audit firm to perform a PCI DSS Report on Compliance (ROC). The audit firm has noted that the merchant's compliance deadline is less than one month away. What should the audit firm do next?

A. File a compliance extension with the PCI Standards Council on behalf of the merchant.

B. Inform the merchant that the ROC can be completed on time.

C. Inform the merchant that the ROC cannot be completed on time and that an extension should be requested.

D. File a compliance extension with the merchant's acquiring bank.

25. An auditor is developing an audit plan for an accounts payable function. Rather than randomly selecting transactions to examine, the auditor wants to select transactions from low, medium, and large payment amounts. Which sample methodology is appropriate for this approach?

A. Judgmental sampling

B. Stratified sampling

C. Nonrandom sampling

D. Statistical sampling

26. A cybersecurity audit firm has completed a penetration test of an organization's web application. The final report contains two findings that indicate the presence of two critical vulnerabilities. The organization disputes the findings because of compensating controls outside the web application interface. How should the audit proceed?

A. The audit firm should remove the findings from the final report.

B. The organization should select another firm to conduct the penetration test.

C. The organization's management should protest the findings and include a letter accompanying the pen test report.

D. The audit firm should permit the customer to include some management comments in the final report.

27. What is the objective of the ISACA audit standard on organizational independence?

A. The auditor's placement in the organization should ensure that the auditor can act independently.

B. The auditor should not work in the same organization as the auditee.

C. To ensure that the auditor has the appearance of independence.

D. To ensure that the auditor has a separate operating budget.

28. An auditor is auditing an organization's risk management process. During the walkthrough, the auditor asked the auditee to list all of the information sources contributing to the process. The auditee cited penetration tests, vendor advisories, nonvendor advisories, and security incidents as inputs. What conclusion should the auditor draw from this?

A. The process is effective because risks are obtained from several disparate sources.

B. The process is ineffective as risk assessments do not occur or contribute to the process.

C. The process is effective because both internal and external sources are used.

D. The process is ineffective because an anonymous tip line was not among the sources.

29. The capability wherein a server is constituted from backup media is known as which type of control?

A. Primary control

B. Manual control

C. Compensating control

D. Recovery control

30. Prior to planning an audit, an auditor would need to conduct a risk assessment to identify high-risk areas in all of the following situations *except*:

- **A.** When a client's most recent risk assessment is two years old
- **B.** When a client's risk assessment does not appear to be adequately rigorous
- **C.** A PCI "Report on Compliance" audit
- **D.** A SOC2 audit

31. Which of the following audit types is appropriate for a financial services provider such as a payroll service?

- **A.** SOC 1
- **B.** SAS70
- **C.** AUP
- **D.** Sarbanes-Oxley

32. Which of the following is the best method for ensuring that an audit project can be completed on time?

- **A.** Distribute a "provided by client" evidence request list at the start of the audit.
- **B.** Prepopulate the issues list with findings likely to occur.
- **C.** Increase the number of auditors on the audit team.
- **D.** Reduce the frequency of status meetings from weekly to monthly.

33. An auditor is about to start an audit of a user account access request and fulfillment process. The audit covers six months, from January through June. The population contains 1,800 transactions. Which of the following sampling methodologies is best suited for this audit?

- **A.** Examine the results of the client's control self-assessment (CSA).
- **B.** Submit some user account access requests and observe how they are performed.
- **C.** Request the first 30 transactions from the auditee.
- **D.** Request the first five transactions from each month in the audit period.

34. An auditor is auditing an organization's personnel onboarding process and examining the background check process. The auditor is mainly interested in whether background checks are performed for all personnel and whether background checks result in no-hire decisions. Which of the following evidence-collection techniques will support this audit objective?

- **A.** Request the full contents of background checks along with hire/no-hire decisions.
- **B.** Request the background check ledger that includes the candidates' names, results of background checks, and hire/no-hire decisions.
- **C.** Request the hire/no-hire decisions from the auditee.
- **D.** Examine the background check process, and note which characteristics of each candidate are included.

35. An auditor wants to audit the changes made to the DBMS configuration of a financial accounting system. What should the auditor use as the transaction population?

- **A.** All of the transactions in the database
- **B.** All of the requested changes in the change management process
- **C.** All of the changes made to the database
- **D.** All of the approved changes in the change management business process

36. A credit card payment processor undergoes an annual PCI DSS Report on Compliance (ROC) audit. What evidence of a passing audit should the payment processor provide to merchant organizations and others?

- **A.** The signed Report on Compliance (ROC)
- **B.** The signed attestation of compliance (AOC)
- **C.** The signed report of validation (ROV)
- **D.** The signed self-assessment questionnaire (SAQ)

37. Which of the following statements about the ISACA Audit Guidelines is correct?

- **A.** ISACA Audit Guidelines apply only to audit firms and not to internal audit departments.
- **B.** ISACA Audit Guidelines are required. Violations may result in fines for violators.
- **C.** ISACA Audit Guidelines are required. Violations may result in loss of certifications.
- **D.** ISACA Audit Guidelines are not required.

38. An external auditor is auditing an organization's third-party risk management (TPRM) process. The auditor has observed that the organization has developed an ISO 27001-based questionnaire sent to all third-party service providers annually. What value-added remarks can the auditor provide?

- **A.** The process can be more efficient if the organization develops risk-based tiers to save time auditing low-risk vendors.
- **B.** The organization should not be sending questionnaires to vendors every year.
- **C.** The organization should structure its questionnaires based on CSA Star.
- **D.** The organization should outsource its third-party management process.

39. What is the difference between SSAE18 Type I and SSAE18 Type II audits?

- **A.** A Type I audit is an audit of process effectiveness, whereas a Type II audit is an audit of process effectiveness and design.
- **B.** A Type I audit is an audit of process design and effectiveness, whereas a Type II audit is an audit of process design.
- **C.** A Type I audit is an audit of process design, whereas a Type II audit is an audit of process design and effectiveness.
- **D.** A Type I audit is an audit of process design and effectiveness, whereas a Type II audit is an audit of process effectiveness.

40. An auditor is auditing the payment systems for a retail store chain that has 80 stores in the region. The auditor needs to observe and take samples from some of the stores' systems. The audit client has selected two stores in the same city as the store chain headquarters and two stores in a nearby town. How should the audit of the store locations proceed?

- **A.** The auditor should learn more about the stores' systems and practices before deciding what to do.
- **B.** The auditor should audit the selected stores and proceed accordingly.
- **C.** The auditor should accept the sampling but select additional stores.
- **D.** The auditor should select which stores to examine and proceed accordingly.

41. As part of an audit of a business process, the auditor has discussed the process with the control owner and the control operators and has collected procedure documents and records related to the process. The auditor is asking internal customers of the business process to describe in their own words how the business process is operated. What kind of evidence collection are these discussions with internal customers?

- **A.** Reconciliation
- **B.** Reperformance
- **C.** Walkthrough
- **D.** Corroborative inquiry

42. Three months after the completion of an audit, the auditor contacted the auditee to inquire about the auditee's activities since the audit and whether the auditee has made any progress related to audit findings. What sort of communication is this outreach from the auditor?

- **A.** The auditor is a good audit partner and wants to ensure that the auditee is successful.
- **B.** The auditor is acting improperly by contacting the auditee outside of an audit and should be censored for unethical behavior.
- **C.** The auditee should assume that the auditor's outreach is personal in nature because this kind of communication is forbidden.
- **D.** The auditor clearly ensures that the auditee is happy with the auditor's work so that the auditor gets next year's audit assignment.

43. According to ISACA Audit Standard 1202, which types of risks should be considered when planning an audit?

- **A.** Fraud risk
- **B.** Business risk
- **C.** Cybersecurity risk
- **D.** Financial risk

44. An IT service desk department that provisions user accounts performs a monthly activity whereby all user account changes in the prior month are checked against the list of corresponding requests in the ticketing system. This activity is known as:

A. An audit

B. A monthly provisioning review

C. A control threat assessment (CTA)

D. A risk assessment

45. An organization that uses video surveillance at a work center has placed visible notices on building entrances that inform people that video surveillance systems are in use. The notices are an example of:

A. Administrative controls

B. Preventive controls

C. Detective controls

D. Deterrent controls

46. An auditor is planning an audit of a financial planning application. Can the auditor rely on a recent application penetration test as a risk-based audit?

A. No, because a penetration test does not reveal risks.

B. No, because a penetration test is not a risk assessment.

C. No: the auditor can make use of the pen test, but a risk assessment is still needed.

D. Yes, because the penetration test serves as a risk assessment in this case.

47. Which of the following is the best example of a control self-assessment of a user account provisioning process?

A. An examination of Active Directory to ensure that only domain administrators can make user account permission changes

B. Checks to see that only authorized personnel made user account changes

C. Confirmation that all user account changes were approved by appropriate personnel

D. Reconciliation of all user account changes against approved requests in the ticketing system

48. The proper sequence of an audit of an accounts payable process is:

A. Identify control owners, make evidence requests, perform walkthroughs, and perform corroborative interviews.

B. Make evidence requests, identify control owners, and perform corroborative interviews.

C. Identify control owners, perform corroborative interviews, make evidence requests, and perform walkthroughs.

D. Perform corroborative interviews, identify control owners, make evidence requests, and perform walkthroughs.

49. An auditor is auditing an accounts payable process and has found no exceptions. The auditor has decided to select additional samples to see whether any exceptions may be found. Which type of sampling is the auditor performing?

A. Stop-or-go sampling

B. Discovery sampling

C. Judgmental sampling

D. Exception sampling

50. Which of the following methods is best suited for an auditee to deliver evidence to an auditor during the audit of a background check process?

A. FTP server

B. Secure file transfer portal

C. Email with SMTP over TLS

D. Courier

51. An auditor has completed an audit, and the deliverable is ready to give to the audit client. What is the best method for delivering the audit report to the client?

A. Courier

B. Secure file transfer portal

C. Email with SMTP over TLS

D. In person, in a close-out meeting

52. What are the potential consequences if an IS auditor is a member of ISACA and CISA certified and violates the ISACA Code of Professional Ethics?

A. Fines

B. Imprisonment

C. Termination of employment

D. Loss of ISACA certifications

53. An auditor is auditing an accounts payable process and has discovered that a single individual has requested and also approved several payments to vendors. What kind of an issue has the auditor found?

A. A separation-of-duties issue

B. A split-custody issue

C. A dual-custodian issue

D. No issue has been identified

54. An organization uses an automated workflow process for request, review, approval, and provisioning of user accounts. Anyone in the organization can request access. Specific individuals are assigned to the review and approval steps. Provisioning is automated. What kind of control is the separation of duties between the review and approval steps?

A. Compensating control

B. Manual control

C. Preventive control

D. Administrative control

55. An auditor is planning an audit of a monthly terminated-users review procedure. The auditor is planning to ask the auditee for a list of current user accounts in Active Directory, as well as a list of current employees and a list of terminated employees from Human Resources so that the auditor can compare the lists. What kind of an audit is the auditor planning to perform?

A. Reperformance

B. Observation

C. Corroboration

D. Walk-back

56. An IT service desk manager is the control owner for the IT department change control process. In an audit of the change control process, the auditor has asked the IT service desk manager to provide all change control tickets whose request numbers end with the digit 6. What sampling methodology has the auditor used?

A. Judgmental sampling

B. Statistical sampling

C. Stratified sampling

D. Stop-or-go sampling

57. An audit firm is planning an audit of an organization's asset management records. For what reason would the auditor request a copy of the entire asset database from the third-party DBA versus a report of assets from the owner of the asset process?

A. Honesty of the evidence provider

B. Objectivity of the evidence provider

C. Independence of the evidence provider

D. Qualification of the evidence provider

58. An auditor has delivered a Sarbanes–Oxley audit report containing 12 exceptions to the audit client, who disagrees with the findings. The audit client is upset and is asking the auditor to remove six findings from the report. A review of the audit findings confirmed that all 12 findings are valid. How should the auditor proceed?

A. Remove the three lowest-risk findings from the report.

B. Remove the six lowest-risk findings from the report.

C. Report the auditee to the Securities and Exchange Commission.

D. Explain to the auditee that the audit report cannot be changed.

59. An auditor has delivered a Sarbanes–Oxley audit report containing 12 exceptions to the audit client, who disagrees with the findings. The audit client is upset and is asking the auditor to remove six findings from the report in exchange for a payment of $25,000. A review of the audit findings confirmed that all 12 findings are valid. How should the auditor proceed?

A. The auditor should report the matter to their manager.

B. The auditor should reject the payment and meet the auditee halfway by removing three of the findings.

C. The auditor should reject the payment and remove six of the findings.

D. The auditor should report the incident to the audit client's audit committee.

60. An auditor is auditing a change control process. During a walkthrough, the control owner described the process as follows: "Engineers plan their changes and send an email about their changes to the IT manager before 5 P.M. on Wednesday. The engineers then proceed with their changes during the change window on Friday evening." What, if any, findings should the auditor identify?

A. The change control process is fine as is but could be improved by creating a ledger of changes.

B. The change control process is fine as is.

C. The change control process lacks a review step.

D. The change control process lacks review and approval steps.

61. An organization utilizes a video surveillance system on all ingress and egress points in its work facility; surveillance cameras are concealed from view, and there are no visible notices. What type of control is this?

A. Administrative control

B. Secret control

C. Detective control

D. Deterrent control

62. An auditor is selecting samples from records in the user access request process. Although privileged access requests account for approximately 5% of all access requests, the auditor wants 20% of the samples to be requests for administrative access. What sampling technique has the auditor selected?

A. Judgmental sampling

B. Stratified sampling

C. Statistical sampling

D. Variable sampling

63. An auditor is auditing a change control process by examining change logs in a database management system and requesting change control records to show that those changes were approved. The auditor plans to proceed until the first exception is found. What sampling technique is being used here?

A. Discovery sampling

B. Stop-or-go sampling

C. Attribute sampling

D. Exception sampling

64. Which of the following is the best description of stop-or-go sampling?

A. The auditor wants to select samples based on arbitrary criteria.

B. The auditor wants to know how many transactions contain a certain range of values.

C. The auditor wants to know the total value of the transaction population.

D. The auditor believes the risk is low and wants to sample as few records as possible.

65. While auditing a payroll process, an auditor intends to keep selecting samples until an error is found. What type of sampling is being performed?

A. Discovery sampling

B. Stop-or-go sampling

C. Attribute sampling

D. Exception sampling

66. A staff auditor is auditing a process, which involves examining the contents of some employee laptop computers. The auditor has detected the presence of child pornography on one laptop computer. What should the auditor do next?

A. Confront the user of the laptop computer.

B. Delete the content from the laptop computer.

C. Notify their supervisor.

D. Notify law enforcement.

67. An audit firm has completed an audit of several auditee business processes. The audit firm is in the process of archiving information for the audit. Which of the following information can be excluded from the archiving process?

A. Field notes

B. Draft audit report

C. Sampled transactions

D. None of these

68. In an external audit of a client organization, one of the staff auditors realizes that their business partner in a side business is one of the auditee managers in the client organization. What should the staff auditor do about this?

A. Maintain professional and ethical behavior during the audit.

B. Refrain from discussing the side business with their business partner during the audit.

C. Notify their supervisor about a potential conflict of interest.

D. Request reassignment to another audit project.

69. An auditor is auditing a release management process by examining policies, procedures, and records and interviewing personnel. The auditor has determined that the personnel who initiate individual software releases are also the approvers. What might the auditor conclude from this?

A. The process appears to have a segregation-of-duties issue.

B. The process appears to have a race condition.

C. The design of the process is appropriate and sound.

D. Nothing can be concluded from this information.

70. An auditor is auditing an organization's vendor risk practices. The information security manager described the process to the auditor, which consists of the security manager performing a security scan of a new vendor's website to measure the level of risk and reaching a conclusion about the vendor's suitability solely based on the scan results. What might the auditor conclude from this?

A. The organization's vendor management risk process is adequate because security scanning is the primary means for identifying risk.

B. The organization's vendor management risk process is inadequate because an objective party should perform the scan.

C. The organization's vendor management risk process is inadequate because the organization should also issue a questionnaire to the vendor.

D. The organization's vendor management risk process is inadequate because it should be performed by an outside party instead of internally.

71. An auditor has completed fieldwork on a customer's SOC 2 audit and has briefed the customer on findings that will appear in the report. What should the customer do next?

A. Challenge the auditor and ask them to prove their findings.

B. Agree with the auditor.

C. Ask for a second opinion from a different partner in the audit firm.

D. Produce management comments that will appear in the published report.

72. Why would an organization's Internal Audit department conduct its own risk assessment versus relying on the risk assessment performed by the Information Security department?

A. The auditor may not believe that the Information Security department is capable of conducting a proper risk assessment.

B. As an objective, independent party, the Internal Audit department should conduct its own risk assessment.

C. The internal auditor is prohibited by law from relying on the Information Security department's risk assessment.

D. The internal auditor would put themselves in a conflict of interest situation.

73. An organization recently hired an experienced cybersecurity leader to make strategic improvements in the organization's cybersecurity capabilities. One item of interest to the cybersecurity leader is the matter of control owner–operators and their commitment to control effectiveness. Which of the following would best serve to improve this commitment?

A. Control self-assessments

B. Security awareness training

C. Penetration testing

D. An external audit

74. To save time in an audit, one of the staff auditors has decided to upload audit findings to a public LLM AI service to direct the service in composing the audit executive summary. The audit manager discovered this practice. What should the audit manager do next?

A. Discipline the staff auditor for compromising the auditee's confidential information.

B. Recognize and reward the staff auditor for innovation and efficiency.

C. Update audit procedures so that other staff auditors will do the same.

D. Notify law enforcement.

75. The director of Internal Audit in a new US-based public company has decided to staff its internal audit with contractors from a public accounting firm. This is an example of:

A. Insourced external audit

B. Outsourced external audit

C. Outsourced internal audit

D. Insourced internal audit

76. When planning an audit, a lead auditor must determine all of the following *except*:

- **A.** Findings
- **B.** Scope
- **C.** Purpose
- **D.** Schedule

77. An organization is required to comply with Sarbanes-Oxley, PCI DSS, ISO 27001, and NIST SP 800-53. What is the best approach for determining how the organization can plan to comply with these?

- **A.** Create separate controls and procedures for each framework.
- **B.** Map all controls together, thus creating the organization's General Computing Controls.
- **C.** Create separate controls, procedures, and records for each framework.
- **D.** Identify the scope for each framework, and map common controls.

78. Two cybersecurity staff members are arguing about the classification of the organization's video surveillance system. One argues that video surveillance is a deterrent control, and the other argues that video surveillance is a detective control. Who is right, and why?

- **A.** Video surveillance is neither deterrent nor detective.
- **B.** Video surveillance is a detective control.
- **C.** Video surveillance is both deterrent and detective.
- **D.** Video surveillance is a deterrent control.

79. An online retail merchant organization with an online product catalog accepts credit card payments from customers but does not store credit card data. A third-party organization accepts payments through a gateway. The CFO argues that the organization is not required to comply with PCI DSS because the organization does not store credit card data. What, if any, are the organization's requirements for complying with PCI DSS?

- **A.** The organization is required to comply because its website directs payments to the third-party payment gateway.
- **B.** The organization is not required to comply because it does not store credit card data.
- **C.** The organization is required to comply because it advertises its acceptance of credit cards for payment.
- **D.** The organization is not required to comply because another organization accepts payments on its behalf.

80. The advantages of control self-assessments include all of the following *except*:

- **A.** Control risks can be identified earlier.
- **B.** Favorable self-assessments can result in audits being delayed.
- **C.** Relationships with control owners can improve through collaboration.
- **D.** More personnel will be aware of the need for effective controls.