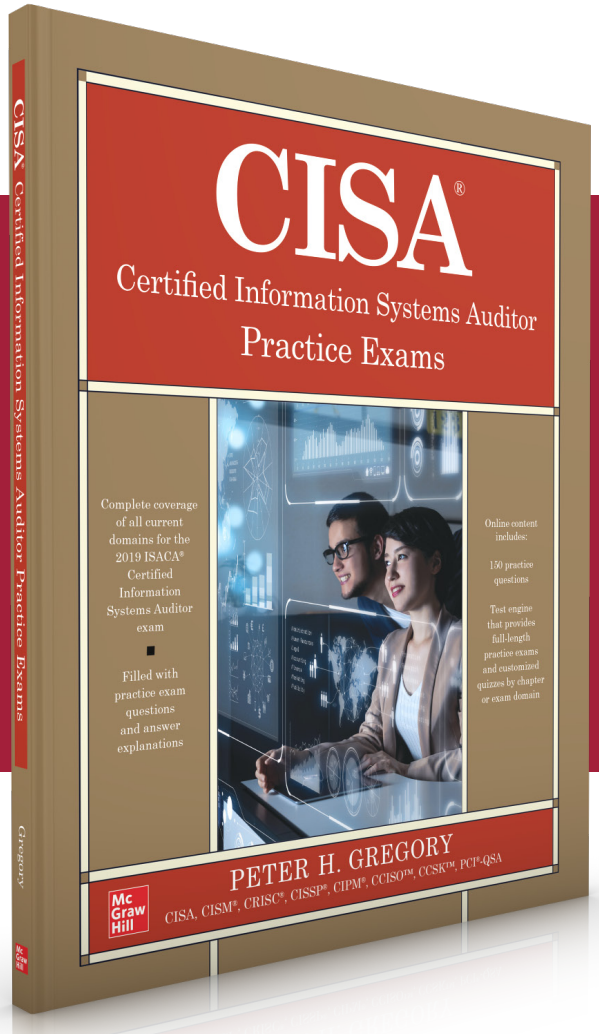
Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

Sample Chapter

CHAPTER 3:
The Audit Process



LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

CHAPTER 3

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 21 percent of the CISA examination.

ISACA defines this domain as follows: "Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives."

The IS audit process is the procedural and ethical structure used by auditors to assess and evaluate the effectiveness of the IT organization and how well it supports the organization's overall goals and objectives. The audit process is backed up by the Information Technology Assurance Framework (ITAF) and the ISACA Code of Professional Ethics. The ITAF is used to ensure that auditors will take a consistent approach from one audit to the next throughout the entire industry. This will help to advance the entire audit profession and facilitate its gradual improvement over time.

LEARN MORE BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

QUESTIONS

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 in an SaaS-based environment to 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.** Compliance audit
   - **B.** Operational audit
   - **C.** Service provider audit
   - **D.** IS audit

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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, while detective controls only record them.
    - **D.** Detective controls stop unwanted events from occurring, while preventive controls only record them.
14. For the purposes of audit planning, can an auditor rely upon 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 himself or herself.
    - **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 to 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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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 from 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. An 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 has discovered the presence of illegal content. What should the staff auditor do next?
    - **A.** Notify law enforcement.
    - **B.** Inform his or her supervisor.
    - **C.** Notify the auditee.
    - **D.** Notify the auditee's audit committee.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

20. A QSA auditor in an audit firm has completed a PCI-DSS audit of a client and has found the client to be noncompliant with one or more PCI-DSS controls. Management in the audit firm has asked the QSA auditor to sign off on 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, but 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 and exits from the data center

B. A visitors 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 U.S.-based organization processes payroll and expense reports in an SaaS-based environment to thousands of corporate customers. Customers outside the United States 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 QSA (PCI) audit firm has been commissioned by a large merchant organization 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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. Non-random 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 the presence of compensating controls outside of 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. Organization's management should protest the findings and include a letter that accompanies the pen test report.

D. The audit firm should permit the customer to have some management comments included 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 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 sources of information that contribute to the process. The auditee cited penetration tests, vendor advisories, non-vendor advisories, and security incidents as all of the 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 apparently 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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* for:
    - **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.** SSAE18
    - **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.** Pre-populate 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 a six-month period 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 is examining the background check process. The auditor is mainly interested in whether background checks are performed for all personnel and whether background check results lead to

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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 for 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 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-based questionnaire that is 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

39. What is the difference between an SSAE18 Type I audit and an SSA18 Type II audit?

- **A.** A Type I audit is an audit of process effectiveness, whereas a Type II audit is an audit of process effectiveness and process design.
- **B.** A Type I audit is an audit of process design and process 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 process 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 that are located 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 a part of an audit of a business process, the auditor has had a discussion with the control owner, as well as the control operators, and has collected procedure documents and records. 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 has 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 a communication is this outreach from the auditor?

- **A.** The auditor is being a good audit partner and wants to ensure 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 since this kind of communication is forbidden.

LEARN MORE BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

D. The auditor is clearly making sure that the auditee is happy with the auditor's work so that the auditor gets the 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 that occurred 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 with 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 penetration test of the application 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. Yes, the auditor can make use of the pen test, but a risk assessment is still needed.

D. Yes, 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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

48. The proper sequence of an audit of an accounts payable process is:
    - **A.** Identify control owners, make evidence requests, perform walkthroughs, do corroborative interviews.
    - **B.** Make evidence requests, identify control owners, do corroborative interviews.
    - **C.** Identify control owners, do corroborative interviews, make evidence requests, perform walkthroughs.
    - **D.** Do 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.** E-mail 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.** E-mail using 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 is CISA certified and violates the ISACA Code of Professional Ethics?
    - **A.** Fines
    - **B.** Imprisonment
    - **C.** Termination of employment
    - **D.** Loss of ISACA certifications

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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 persons 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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

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 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 any six findings from the report. A review of the audit findings resulted in the confirmation that all 12 findings are valid. How should the auditor proceed?

- **A.** Remove the three lowest-risk findings from the report.
- **B.** Remote 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 any six findings from the report in exchange for a payment of $25,000. A review of the audit findings resulted in the confirmation that all 12 findings are valid. How should the auditor proceed?

- **A.** The auditor should report the matter to his or her 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 e-mail 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

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. While privileged access requests account for approximately 5 percent of all access requests, the auditor wants 20 percent 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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

QUICK ANSWER KEY

1. C	22. A	43. B
2. B	23. C	44. B
3. A	24. C	45. D
4. C	25. B	46. C
5. C	26. D	47. D
6. A	27. A	48. A
7. D	28. B	49. B
8. B	29. D	50. B
9. C	30. C	51. D
10. D	31. A	52. D
11. A	32. A	53. A
12. D	33. D	54. C
13. C	34. B	55. A
14. B	35. C	56. B
15. D	36. B	57. C
16. D	37. D	58. D
17. A	38. A	59. A
18. C	39. C	60. D
19. B	40. A	61. C
20. A	41. D	62. B
21. D	42. A	63. A

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

ANSWERS 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

   ☑ **C.** The IT Assurance Framework is an ISACA publication that includes the ISACA Code of Professional Ethics, IS audit and assurance standards, IS audit and assurance guidelines, and IS audit and assurance tools and techniques. It does not contain the ISACA Audit Job Practice.

   ☒ **A** is incorrect because the ITAF does include the ISACA Code of Professional Ethics.

   ☒ **B** is incorrect because the ITAF does include IS audit and assurance standards.

   ☒ **D** is incorrect because the ITAF does include 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.

   ☑ **B.** The CAB should be discussing emergency changes that were made since the last CAB meeting. While the changes were already made, they should go through a similar approval process to ensure that all stakeholders are aware of the changes and that they agree that the changes made were appropriate.

   ☒ **A** is incorrect because a change control process needs to address all changes, including planned changes and emergency changes.

   ☒ **C** is incorrect because emergency changes are often necessary to counteract the effects of unexpected downtime, capacity issues, and other matters.

   ☒ **D** is incorrect because the change control process should address all changes, both planned future changes and recent 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

LEARN MORE BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **A.** A video surveillance system is considered a detective control because it only records events without actually preventing events such as controls like locked doors and other barriers. A video surveillance system, when its components are conspicuous, is also considered a deterrent control, because its obvious presence serves as a visible deterrent to persons who may be considering an intrusion into a building.

☒ **B** is incorrect because a visible video surveillance system is not considered *only* as a detective control but also as a deterrent control. If the video surveillance system's components are hidden from view, then it would be considered only a detective control.

☒ **C** is incorrect because a visible working video surveillance system is not considered *only* a deterrent control but also a detective control since it would record wanted and unwanted events. If the video surveillance system was fake or inoperative, only then would it be considered solely a deterrent control.

☒ **D** is incorrect because a video surveillance system is never considered a preventive control since it does not actually prevent unwanted events, as does a locked entrance.

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

☑ **C.** A risk assessment is the primary means for determining which controls may represent greater risk to the organization.

☒ **A** is incorrect because an incident log will not reveal all types of risks. Further, if the incident detection and response processes are ineffective, then the incident log could provide a false sense of security.

☒ **B** is incorrect because there may have been changes in operations since the prior audit that only a risk assessment would reveal.

☒ **D** is incorrect because performance metrics would probably not reveal enough information about risks in controls.

5. An organization processes payroll and expense reports in an SaaS-based environment to 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. Compliance audit

B. Operational audit

C. Service provider audit

D. IS audit

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **C.** A service provider audit, such as an SSAE18, SOC2, ISO 27001 certification, or AUP audit, is designed for service providers that want to provide objective assurance of the integrity of their control environment.

☒ **A** is incorrect because a compliance audit is used to ensure that an organization is in compliance with specific laws, regulations, or standards.

☒ **B** is incorrect because an operational audit is an audit that is performed for internal use. This is a potential answer, but not the best answer.

☒ **D** is incorrect because an IS audit is an audit that is performed for internal use. This is a potential answer, but not the best answer.

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

☑ **A.** While any of these answers is plausible, the first thing that should be examined is whether the audit is being effectively project managed, so that all parties understand the audit's objectives, schedule, resources required, and regular status reporting.

☒ **B** is incorrect. While plausible, there isn't enough information here to draw this conclusion.

☒ **C** is incorrect. While plausible, there isn't enough information here to draw this conclusion.

☒ **D** is incorrect. While plausible, there isn't enough information here to draw this conclusion.

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

☑ **D.** In an audit where an auditor needs to select a portion of events to test, statistical sampling is the best approach.

☒ **A** is incorrect because the auditor is not examining individual transactions to determine whether each should be included in the sampling.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☒ **B** is incorrect because "random sampling" may be a common vernacular for this approach, but this is not the official ISACA term for it.

☒ **C** is incorrect because stratified sampling involves selecting samples from various portions of the population.

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

☑ **B.** An auditor generally will examine process documentation first to understand how a process is supposed to be performed. This will be followed by a walkthrough, observation, examination of records, and corroborative inquiry (and often in that sequence).

☒ **A** is incorrect because an auditor will generally first want to read process documentation before watching personnel perform tasks.

☒ **C** is incorrect because an auditor will generally first want to read process documentation before performing a walkthrough.

☒ **D** is incorrect because an auditor will generally want to examine a process thoroughly before performing a 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.

☑ **C.** The task of auditing a large number of transactions needs to be automated with one or more computer-assisted audit techniques (CAATs). Manually testing a large number of transactions would be onerous and costly.

☒ **A** is incorrect because the volume of transactions is too high to consider reperforming them manually.

☒ **B** is incorrect because this approach would require excessive manual effort.

☒ **D** is incorrect because it is not the best answer. This approach might be the best alternative, however, but the auditor would have to develop techniques to analyze the data.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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.

☑ **D.** There is rarely a valid reason why the audit client should not be notified right away of an audit exception. That said, often the auditor will need to reserve the final audit opinion until all of the testing has been completed and all of the audit exceptions analyzed. Still, notifying the audit client of individual exceptions during the audit provides the audit client with opportunities to begin remediation.

☒ **A** is incorrect because an audit committee is not always the audit client.

☒ **B** is incorrect because there is rarely a valid reason for waiting until the final audit report to inform an audit client of audit exceptions.

☒ **C** is incorrect because this is not the best answer; this is a valid alternative, however.

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.

☑ **A.** ISACA Audit Standards are mandatory for all audit professionals—compliance with ISACA Audit Standards is a condition for earning and retaining the CISA certification.

☒ **B** is incorrect because ISACA Audit Standards are not optional for CISA certification holders.

☒ **C** is incorrect because ISACA Audit Guidelines are not mandatory, but instead serve as helpful guidelines for the implementation of ISACA Audit Standards.

☒ **D** is incorrect because ISACA Audit Standards are mandatory for all audits. That said, often there are additional audit standards for specific types of audits, such as Sarbanes-Oxley (SOX), PCI-DSS, SSAE18, and others.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

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

☑ **D.** The problem with the existing business process can be partly remedied by a frequent user access review, which will partly compensate for the control failures. However, the organization should seek to identify and correct the root cause(s) of the control failures so that there are fewer exceptions identified in the monthly user access reviews as well as in subsequent audits.

☒ **A** is incorrect because the problem with this process is not whether the right approvers are involved, but that user accesses are being granted through bypassing the request process altogether.

☒ **B** is incorrect because the problem with this process is not whether the right approvers are involved, but that user accesses are being granted through bypassing the request process altogether.

☒ **C** is incorrect because an annual user access review is too infrequent for this situation.

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, while detective controls only record them.

D. Detective controls stop unwanted events from occurring, while preventive controls only record them.

☑ **C.** The best and first approach to unwanted events is prevention. Where prevention is difficult or expensive, detection is the next best approach.

☒ **A** is incorrect because preventive controls are not necessarily easier to justify or implement.

☒ **B** is incorrect because preventive controls are not necessarily less expensive to implement.

☒ **D** is incorrect because detective controls do not prevent events.

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

A. Yes, in all cases.

B. Yes, if the risk assessment was performed by a qualified external entity.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

C. No. The auditor must perform a risk assessment himself or herself.

D. No. The auditor does not require a risk assessment to develop an audit plan.

☑ **B.** An auditor can use a risk assessment performed by a qualified external party to develop a risk-based audit plan. This will result in areas of higher risk being examined more closely than areas of lower risk.

☒ **A** is incorrect because there are certainly cases where an auditor cannot use a client's risk assessment—for example, if the client's risk assessment was performed by unqualified persons or if there were signs of bias.

☒ **C** is incorrect because it is not always necessary for an auditor to perform the audit himself or herself. Often an external risk assessment can be used, provided it is sound.

☒ **D** is incorrect because a risk assessment will result in a better audit plan that is risk-aligned.

15. An organization processes payroll and expense reports in an SaaS-based environment to 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

☑ **D.** The payroll services organization should undertake an SSAE18 audit. This type of audit is designed for financial services providers so that the auditors of the customers of the payroll services organization can rely on the payroll services organization's SSAE18 audit report in the course of auditing financial controls.

☒ **A** is incorrect because an AUP audit is not the best choice. This is a viable alternative, however, in the event the organization decides not to undertake an SSAE18 audit.

☒ **B** is incorrect because a PA-DSS audit is an audit of a commercial credit card payment application.

☒ **C** is incorrect because a PCI-DSS audit is an audit of an organization's credit card data processing environment.

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 from randomly selected servers from the systems engineer.

D. Capture screenshots from randomly selected servers during a walkthrough with the systems engineer.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **D.** The auditor should select which servers are to be sampled (by whatever sampling methodology) and view the configurations during a walkthrough with a systems engineer. This is the most reliable method for ensuring the integrity of the evidence.

☒ **A** is incorrect because the systems engineer should not be permitted to select the servers to be sampled; the systems engineer could deliberately avoid servers known to violate the policy.

☒ **B** and **C** are incorrect because the auditor cannot be sure that the requested screenshots actually correspond to the servers selected.

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

☑ **A.** The auditor wants to examine the population and select specific high-risk transactions.

☒ **B** is incorrect because some of the transactions are not being randomly selected, and because "random sampling" is not the official term for this technique.

☒ **C** is incorrect because this is not an example of stratified sampling.

☒ **D** is incorrect because some of the transactions are not being randomly selected.

18. An auditor is auditing an organization's user account request and fulfillment process. An 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

☑ **C.** A control owner describing a process is known as a walkthrough. Here, each step of a process is described in detail to the auditor.

☒ **A** is incorrect because observation refers to an auditor watching personnel perform the process.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☒ **B** is incorrect because document review generally consists of the auditor reading the document on his or her own, away from the presence of the control owner. Document review usually precedes a walkthrough.

☒ **D** is incorrect because corroborative inquiry usually takes place after a walkthrough and after examining records.

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 has discovered the presence of illegal content. What should the staff auditor do next?

A. Notify law enforcement.

B. Inform his or her supervisor.

C. Notify the auditee.

D. Notify the auditee's audit committee.

☑ **B.** The staff auditor should first notify his or her supervisor, who in turn may notify others in the audit firm. Depending upon the nature of the illegal content, it may be appropriate for the audit firm to notify law enforcement, the auditee, or senior officials in the auditee organization, such as audit committee members. Local laws and regulations may influence this decision.

☒ **A** is incorrect because this may not be the best next step, depending on local laws and regulations. In most cases, it's best to notify one's supervisor, who in turn will discuss the matter with others in the audit firm.

☒ **C** is incorrect because the auditee could be the person responsible for placing the illegal content on the storage system. Notifying this person could give them an opportunity to quickly remove the content before law enforcement is able to examine the storage system.

☒ **D** is incorrect because the audit committee is not necessarily the appropriate party to notify first. Depending upon local laws and regulations, law enforcement may need to be notified. The best course of action is for the auditor to notify his or her supervisor, who can then assemble individuals in the audit firm who can decide the appropriate course of action.

20. A QSA auditor in an audit firm has completed a PCI-DSS audit of a client and has found the client to be noncompliant with one or more PCI-DSS controls. Management in the audit firm has asked the QSA auditor to sign off on 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, but under duress.

C. Sign the audit report as compliant.

D. Notify the audit client of the matter.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **A.** The QSA auditor signing the audit report as compliant would be a violation of the ISACA Code of Professional Ethics. Were ISACA to learn about this matter, the auditor could lose his or her ISACA certifications.

☒ **B** is incorrect because this may still jeopardize the auditor's standing with the ISACA Code of Professional Ethics.

☒ **C** is incorrect because this would be a clear violation of the ISACA Code of Professional Ethics, and the auditor could lose his or her ISACA certifications.

☒ **D** is incorrect because this may cause confusion or anger on the part of the auditee organization.

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).

☑ **D.** Control self-assessments (CSAs) force control owners to focus on the effectiveness of their controls. For the most part, control owners will self-regulate and make improvements to their control procedures in order to ensure that their controls are more effective.

☒ **A** is incorrect because signing a document will not necessarily compel control owners to take ownership of their controls in the same way a CSA would.

☒ **B** and **C** are incorrect. While an audit would highlight control deficiencies, a CSA is a more effective means for control owners to pay attention to the effectiveness of their controls by forcing them to evaluate them.

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 and exits from the data center

B. A visitors 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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **A.** A video surveillance system would record all persons entering and leaving the data center. A security manager could examine the video contents from time to time to understand whether there are specific persons who violate the policy.

☒ **B** is incorrect because visitors who know they are not authorized to enter the data center are unlikely to sign the visitor log.

☒ **C** is incorrect because a man trap, while effective, is a costly control. It may ultimately prove necessary if review of video surveillance and disciplinary action do not resolve the matter.

☒ **D** is incorrect because visitors who know they are not authorized to enter the data center are not likely to conform to the policy; further, if they are outsiders, they may not be aware of the policy.

23. A U.S.-based organization processes payroll and expense reports in an SaaS-based environment to thousands of corporate customers. Customers outside the United States 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

☑ **C.** An ISAE3402 audit is the international version of the SSAE18 audit.

☒ **A** is incorrect because, while valuable, an ISO/IEC 27001 audit is not the best choice. An ISO audit would cover a broad spectrum of security controls but no financially specific controls.

☒ **B** is incorrect because a SOC2 audit is a general-purpose audit of a service provider, but it lacks financially specific controls.

☒ **D** is incorrect because an SSAE18 audit is technically valid only within the United States.

24. A QSA (PCI) audit firm has been commissioned by a large merchant organization 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **C.** There is little hope that the ROC can be completed in four weeks. After being notified by the audit firm, the merchant organization should request an extension of its acquiring bank.

☒ **A** is incorrect because a QSA firm does not file extensions on behalf of its audit clients.

☒ **B** is incorrect because it is unlikely that the ROC can be completed in four weeks. A PCI-DSS audit of a large merchant organization is sure to take several weeks from start to finish.

☒ **D** is incorrect because QSA firms do not file extensions of behalf of their audit clients.

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. Non-random sampling

D. Statistical sampling

☑ **B.** Stratified sampling involves selecting samples based on some quantified value in each sample (in this case, the payment amount). Stratified sampling is useful for situations like this where auditors want to be sure to examine very high- or very low-value samples that might not be selected in random sampling.

☒ **A** is incorrect because judgmental sampling is, by definition, not random. However, this would be the next best choice.

☒ **C** is incorrect because non-random sampling is not a sampling methodology.

☒ **D** is incorrect because statistical sampling might not capture enough of the high- or low-value transactions if there are too few of these.

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 the presence of compensating controls outside of 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. Organization's management should protest the findings and include a letter that accompanies the pen test report.

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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **D.** Management's comments will appear in the report where the specific findings are discussed.

☒ **A** is incorrect because the audit firm should not remove a finding simply because the audit client disagrees with it.

☒ **B** is incorrect because this may not be a viable option for cost and scheduling reasons.

☒ **C** is incorrect because a separate management letter would be seen in a more negative light. However, this may be the organization's best option if the audit firm is unwilling to include 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 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.

☑ **A.** ISACA audit standard 1002, "Organizational Independence," states the following: "The IS auditor's placement in the command-and-control structure of the organization should ensure that the IS auditor can act independently." This helps to avoid the possibility that the auditor is being coerced into providing a favorable audit opinion.

☒ **B** is incorrect because the audit standard does not require the auditor to work in a different organization. Indeed, internal audit departments in U.S. public companies are a part of the organization.

☒ **C** is incorrect because it is important to not only ensure the *appearance* of independence but the *fact* of independence.

☒ **D** is incorrect because a separate budget does not necessarily equate to independence.

28. An auditor is auditing an organization's risk management process. During the walkthrough, the auditor asked the auditee to list all of the sources of information that contribute to the process. The auditee cited penetration tests, vendor advisories, non-vendor advisories, and security incidents as all of the 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 apparently 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **B.** The absence of risk assessments (or their omission as an input to the risk management process) constitutes an ineffective process. Risk assessments are among the most important input to the risk management process.

☒ **A** and **C** are incorrect because the process cannot be viewed as effective in the absence of risk assessments.

☒ **D** is incorrect because an anonymous tip line, while important, is not considered a key information source for a risk management process.

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

☑ **D.** Restoration of a server from backup media is known as a recovery control.

☒ **A** is incorrect because "primary" is not considered a class of control.

☒ **B** is incorrect because while recovering a server may be manual, it could also be automated. Rebuilding a server from backup is generally considered a recovery control.

☒ **C** is incorrect because rebuilding a server is generally not considered a compensating 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* for:

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

☑ **C.** The PCI audit is not risk-based, and the presence or absence of a risk assessment will not alter the audit plan. This is despite the fact that PCI (as of version 3.2.1) requires an organization to conduct a risk assessment, although this has no bearing on the organization's obligation to implement all controls in the standard.

☒ **A, B,** and **D** are incorrect because these are valid reasons that would compel an auditor to conduct a risk assessment prior to developing the audit plan.

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

A. SSAE18

B. SAS70

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

C. AUP

D. Sarbanes-Oxley

☑ **A.** An SSAE18 audit is specifically intended for financial service providers such as payroll, general accounting, expense management, and other financial services.

☒ **B** is incorrect because the SAS70 audit standard has been deprecated and replaced by the SSAE18 standard.

☒ **C** is incorrect because an AUP audit is general purpose in nature and not specifically designed for financial services.

☒ **D** is incorrect because a Sarbanes-Oxley audit is intended for the financial business processes of a U.S. public company.

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. Pre-populate 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.

☑ **A.** Auditees sometimes take quite a long time to search for and provide requested evidence to auditors. By providing this request list at the beginning of the audit, auditors will obtain evidence earlier than if they wait until their walkthrough meetings.

☒ **B** is incorrect because this is not an accepted practice, and it would not save much time even in circumstances where auditors were sure that certain exceptions were going to occur.

☒ **C** is incorrect because it may not be feasible to increase the size of the audit team. Besides, the number of auditors is not always the factor that determines the duration of an audit.

☒ **D** is incorrect because reducing audit status meetings from weekly to monthly could have the opposite effect and increase the time for an audit project to complete, because of reduced communication.

33. An auditor is about to start an audit of a user account access request and fulfillment process. The audit covers a six-month period 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

☑ **D.** This methodology captures transactions through the entire audit period. In a period of this length, there could be personnel changes and other changes that could result in instances of acceptable or unacceptable performance throughout the period.

☒ **A** is incorrect because an auditee's CSA might not be of sufficient integrity to be relied upon. Further, specific audit rules or standards might preclude the use of a CSA.

☒ **B** is incorrect because reperformance assesses the current effectiveness of a control, not whether the control was effective throughout the audit period.

☒ **C** is incorrect because this will assess the process only at the beginning of the six-month audit period. If the process was effective in January but ineffective for the rest of the period, this technique would conceal this possibility.

34. An auditor is auditing an organization's personnel onboarding process and is examining the background check process. The auditor is mainly interested in whether background checks are performed for all personnel and whether background check results lead to 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 for each candidate are included.

☑ **B.** This evidence request will provide enough information for the auditor to understand whether background checks are performed for all positions requiring it, as well as whether any no-hire decisions are made.

☒ **A** is incorrect because the auditor should not need to see the details of individuals' background checks. This is highly sensitive information.

☒ **C** is incorrect because this does not reveal the correlation between pass/no-pass results and hire/no-hire decisions.

☒ **D** is incorrect because this audit requires examination of records, not just examination of the business process.

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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **C.** The total population is the total set of configuration changes present in the DBMS.

☒ **A** is incorrect because this would include all financial transactions, which is far larger than the desired population.

☒ **B** is incorrect because this would not include changes made to the system that were not requested.

☒ **D** is incorrect because this would not include changes made to the system that were not approved or requested.

36. A credit card payment processor undergoes an annual PCI 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)

☑ **B.** It is entirely sufficient for the service provider to provide the signed attestation of compliance (AOC) to any merchant, customer, or other entity requesting evidence of PCI compliance.

☒ **A** is incorrect because the service provider should not need to provide the entire ROC, as this would provide excessive details of its internal operations. The AOC contains sufficient information regarding the pass or fail status of the audit and its PCI compliance.

☒ **C** is incorrect, as an ROV was not performed.

☒ **D** is incorrect because an SAQ was not completed.

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.

☑ **D.** ISACA Audit Guidelines are suggested implementation guidelines and not required of ISACA-certified personnel.

☒ **A** is incorrect because ISACA Audit Guidelines apply in all auditing situations.

☒ **B** and **C** are incorrect because ISACA Audit Guidelines are optional and not required.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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-based questionnaire that is 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.

☑ **A.** The TPRM process could indeed be more efficient if the organization stratifies its vendors based on risk. The highest-risk vendors would be assessed annually with the most rigorous questionnaire, while vendors at lower-risk tiers would be assessed with shorter questionnaires or not at all.

☒ **B** is incorrect because the organization should be sending questionnaires to its high-risk vendors annually.

☒ **C** is incorrect, as an ISO-based questionnaire may very possibly be sufficient.

☒ **D** is incorrect because there is no indication that suggests the TPRM process should be outsourced.

39. What is the difference between an SSAE18 Type I audit and an SSA18 Type II audit?

A. A Type I audit is an audit of process effectiveness, whereas a Type II audit is an audit of process effectiveness and process design.

B. A Type I audit is an audit of process design and process 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 process 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.

☑ **C.** This is the correct definition of SSAE18 Type I and Type II audits.

☒ **A, B,** and **D** are incorrect because these are incorrect definitions of SSAE18 Type I and Type II audits.

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 that are located 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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.

☑ **A.** While the auditee's desire to select the stores to audit may seem proactive, the auditor needs to better understand the nature of each store's information systems before overruling the auditee. For instance, the systems in all stores may be identically configured, and the nearby store operators may be better equipped to explain audit processes. On the other hand, if store systems were not identically configured and operated, the client's desire to select samples may have to be overruled, so that the auditor retains independence in fact.

☒ **B** is incorrect. There may be reasons why the auditee selected the nearby stores; among them, their processes may be more disciplined than others that are farther away. Unless the auditor is confident that all stores' systems are identical, the auditor must select samples himself or herself.

☒ **C** is incorrect because there may be impropriety involved on the part of the auditee's desire to select samples.

☒ **D** is incorrect. However, if the auditor is unable to conclude that all stores' information systems are identically configured and run, he or she must select the samples.

41. As a part of an audit of a business process, the auditor has had a discussion with the control owner, as well as the control operators, and has collected procedure documents and records. 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

☑ **D.** An auditor having discussions about a business process with additional personnel outside the process is known as corroborative inquiry. This helps to give the auditor more confidence in the veracity of the evidence obtained from control owners and operators.

☒ **A** is incorrect because there is no audit collection technique known as reconciliation.

☒ **B** is incorrect because reperformance is defined as the auditor performing some of the control procedure himself or herself, such as recalculating a batch total.

☒ **C** is incorrect because a walkthrough is performed by the control owner or operator, who describes the business process to the auditor.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

42. Three months after the completion of an audit, the auditor has 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 a communication is this outreach from the auditor?

A. The auditor is being a good audit partner and wants to ensure 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 since this kind of communication is forbidden.

D. The auditor is clearly making sure that the auditee is happy with the auditor's work so that the auditor gets the next year's audit assignment.

☑ **A.** An auditor is free to contact an auditee after an audit to show concern for the auditee and be sure that the auditee is proceeding properly by working to resolve any findings identified by the auditor.

☒ **B** is incorrect, as the auditor is not acting improperly.

☒ **C** is incorrect, as the auditor is within his or her professional bounds to communicate with the auditee after the audit. In many cases, auditors are encouraged in this regard.

☒ **D** is incorrect because it is indeed hoped that the auditor is not "fishing for business" by feigning interest in the auditee's well-being.

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

☑ **B.** All types of risks should be considered when planning an audit of a business process or system.

☒ **A** is incorrect because fraud risk is not the only risk that should be considered.

☒ **C** is incorrect, as cybersecurity risk is only one type of risk that should be considered.

☒ **D** is incorrect because financial risk is only one type of risk that should be considered.

44. An IT service desk department that provisions user accounts performs a monthly activity whereby all user account changes that occurred 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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

C. A control threat-assessment (CTA)

D. A risk assessment

☑ **B.** The service desk is performing a monthly review of user account provisioning to make sure that all such account provisioning activities were in fact requested.

☒ **A** is incorrect because this activity is not an audit, because the service desk is checking its own work.

☒ **C** is incorrect because threats are not being analyzed in this activity.

☒ **D** is incorrect because this activity is not a risk assessment, but an activity review.

45. An organization with 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

☑ **D.** Visible notices announcing its presence is an example of a deterrent control.

☒ **A** is incorrect because visible notes are not examples of administrative controls. An example of an administrative control is a policy.

☒ **B** is incorrect because neither video surveillance nor visible notices are preventive controls. An example of a preventive control is a locked door.

☒ **C** is incorrect. While video surveillance itself is a detective control, a visible notice announcing video surveillance is a deterrent control.

46. An auditor is planning an audit of a financial planning application. Can the auditor rely on a recent penetration test of the application 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. Yes, the auditor can make use of the pen test, but a risk assessment is still needed.

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

☑ **C.** A penetration test reveals a limited view of risks, although a full risk assessment is still needed if the audit is to be truly risk-driven.

☒ **A** is incorrect because penetration tests do reveal some risks.

☒ **B** is incorrect. While it is true that a penetration test is not a risk assessment, the auditor can still rely upon it in order to have a partial view of risk.

☒ **D** is incorrect because a penetration test is never considered a full risk assessment.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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

☑ **D.** A reconciliation of all user account changes with approved requests in the ticketing system ensures that all such changes were actually requested and approved.

☒ **A** is incorrect. Confirmation that only domain administrators can make user account changes does not reveal whether the user account provisioning process is effective.

☒ **B** is incorrect. Checks to see that only authorized personnel made user account changes does not reveal whether the user account provisioning process is effective.

☒ **C** is incorrect. Checking whether the approvers of user account changes were appropriate does not reveal whether the process is effective.

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

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

B. Make evidence requests, identify control owners, do corroborative interviews.

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

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

☑ **A.** It is necessary to identify control owners so that evidence requests can be sent to the right personnel. Next, walkthroughs are performed, and finally corroborative interviews are held.

☒ **B** is incorrect. If control owners are not first identified, evidence requests will be sent to the wrong personnel.

☒ **C** is incorrect. Corroborative interviews are performed after walkthroughs.

☒ **D** is incorrect. Corroborative interviews are performed after evidence requests and 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

LEARN MORE BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

C. Judgmental sampling

D. Exception sampling

☑ **B.** Discovery sampling is used when an auditor is examining samples in the search for at least one exception.

☒ **A** is incorrect because stop-or-go sampling is used when the auditor feels there is a low risk of finding exceptions.

☒ **C** is incorrect because this is not judgmental sampling.

☒ **D** is incorrect because there is no such thing as 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. E-mail with SMTP over TLS

D. Courier

☑ **B.** A secure file transfer portal is the best choice, because sensitive information will be encrypted in transit, end to end, and can handle volumes of evidence that may be too large to e-mail.

☒ **A** is incorrect because an FTP server is not considered secure, since neither login credentials nor data in transit is encrypted.

☒ **C** is incorrect for two reasons. First, the evidence could well be too large to send over e-mail; second, SMTP over TLS only encrypts e-mail between mail servers, not end to end.

☒ **D** is incorrect because using a courier is inefficient, as evidence would first have to be printed and electronic analysis of the evidence would not be possible.

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. E-mail using SMTP over TLS

D. In person, in a close-out meeting

☑ **D.** The best way to deliver an audit report is face to face, so that the auditor can explain the audit project, provide the audit report, and answer any questions that the audit client might have. An in-person meeting provides the auditor with valuable body language cues from the audit client so that the auditor will better understand the audit client's response to the audit report and its description of findings.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☒ **A** is incorrect because courier delivery does not provide an opportunity for a face-to-face discussion of the audit project and its results.

☒ **B** is incorrect because e-mail delivery does not provide an opportunity for a face-to-face discussion of the audit project and its results.

☒ **C** is incorrect because a secure file transfer portal does not provide an opportunity for a face-to-face discussion of the audit project and its results.

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

A. Fines

B. Imprisonment

C. Termination of employment

D. Loss of ISACA certifications

☑ **D.** An ISACA member violating the ISACA Code of Professional Ethics "can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures," including loss of certifications.

☒ **A** is incorrect because fines are not a part of ISACA disciplinary action. However, if the matter also includes the violation of laws, there may be fines levied in that case.

☒ **B** is incorrect because imprisonment is not a part of ISACA disciplinary action. However, if the situation also includes the violation of laws, imprisonment is a possible outcome.

☒ **C** is incorrect, unless the matter is also seen as egregious by the IS auditor's employer, who may need to terminate the auditor's employment.

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.

☑ **A.** The auditor has discovered a separation of duties (sometimes known as segregation of duties) issue. Payment request and approval should be handled by separate persons in accounts payable.

☒ **B** is incorrect because this is not a split custody issue, but a separation of duties issue.

☒ **C** is incorrect because this is not a dual custodian issue.

☒ **D** is incorrect because the auditor's discovery is indeed an audit exception.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

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 persons 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

☑ **C.** This is a preventive control and also an automatic control. The workflow prevents a single individual from performing both the review and approval steps.

☒ **A** is incorrect because this is not a compensating control, but a preventive control.

☒ **B** is incorrect because this is not a manual control, but preventive and automatic.

☒ **D** is incorrect because this is not an administrative control. There may indeed be a policy that requires the separation of duties (and the policy would be an administrative control), but the implementation of the control in the workflow system is a preventive 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

☑ **A.** Since the auditor is going to be essentially repeating the steps performed in the review, this is a reperformance audit.

☒ **B** is incorrect because the auditor is not observing the auditee perform the review.

☒ **C** is incorrect because the auditor is not interviewing additional parties to obtain corroborative evidence of the process.

☒ **D** is incorrect because "walk-back" is not a type of audit.

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

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **B.** This is statistical sampling, where the auditor has requested 10 percent of the population, effectively random and spread throughout the audit period. This assumes, of course, that change control requests are serialized sequentially.

☒ **A** is incorrect because this is not judgmental sampling. Judgmental sampling occurs when an auditor is examining items in a population and using professional judgement to determine whether to include a specific item in the sample.

☒ **C** is incorrect because this is not stratified sampling. Stratified sampling occurs when an auditor selects items in various numeric ranges (such as purchase orders of high amounts and low amounts).

☒ **D** is incorrect because this is not stop-or-go sampling. Stop-or-go sampling is used when an auditor is confident there will be few or no exceptions and decides to stop sampling early.

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 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

☑ **C.** The DBA is an independent party from the asset process owner and has little or no interest in the outcome of the audit.

☒ **A** is incorrect because an auditor is not likely to suspect the honesty of a process owner.

☒ **B** is incorrect because this is not the best answer.

☒ **D** is incorrect because the DBA and asset process owner are both qualified to provide evidence.

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 any six findings from the report. A review of the audit findings resulted in the confirmation that all 12 findings are valid. How should the auditor proceed?

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

B. Remote 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.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☑ **D.** The auditor has no choice but to stand by the audit report as is, particularly after a review upholds all findings.

☒ **A** and **B** are incorrect because the auditor cannot compromise himself or herself in this way.

☒ **C** is incorrect because this matter does not warrant reporting to the authorities. If the audit client was offering a bribe, then perhaps notifying the authorities would be more appropriate.

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 any six findings from the report in exchange for a payment of $25,000. A review of the audit findings resulted in the confirmation that all 12 findings are valid. How should the auditor proceed?

A. The auditor should report the matter to his or her 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.

☑ **A.** The auditor should first report the matter to his or her manager, who will in turn decide how to handle it. More than likely, the audit manager will notify the audit client's audit committee, who can decide to refer the matter to regulatory authorities.

☒ **B** and **C** are incorrect because the auditor should stand by the report and not make any changes to it.

☒ **D** is incorrect because a better course of action is to first notify his or her manager, who will decide how to handle the matter further.

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 e-mail 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.

☑ **D.** The change control process lacks a step where requested changes are reviewed, discussed, and approved. As it stands, it appears that engineers unilaterally decide what changes to make.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

☒ **A** is incorrect because the process lacks an approval step.

☒ **B** is incorrect because the process should include an approval step.

☒ **C** is incorrect because the more important finding is the lack of an approval step.

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

☑ **C.** This is a detective control. The system is not a deterrent control, since the video surveillance system is not visible.

☒ **A** is incorrect because an example of an administrative control is a policy or standard.

☒ **B** is incorrect because controls are not typically classified as "secret."

☒ **D** is incorrect because this particular video surveillance control is not a deterrent control, since the cameras are not visible.

62. An auditor is selecting samples from records in the user access request process. While privileged access requests account for approximately 5 percent of all access requests, the auditor wants 20 percent 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

☑ **B.** This is stratified sampling, where an auditor is selecting samples from various classes or values—in this case, higher-risk privileged accounts.

☒ **A** is incorrect because the auditor is not examining samples to be selected.

☒ **C** is incorrect because statistical sampling would result in about 5 percent of the selected samples being related to privileged access requests.

☒ **D** is incorrect because variable sampling is used to estimate conclusions about the evidence population.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill

Mc Graw Hill

CISA®
Certified Information Systems Auditor
Practice Exams

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

☑ **A.** This is an example of the discovery sampling technique, where an auditor examines samples until an exception is found.

☒ **B** is incorrect because stop-or-go sampling is a technique where an auditor will stop selecting samples when he or she determines that the risk is low enough.

☒ **C** is incorrect because attribute sampling is a technique where an auditor is trying to determine how many of different types of samples exist.

☒ **D** is incorrect because "exception sampling" is not a standard sampling technique.

LEARN MORE

BUY NOW

Because learning changes everything.®

©2020 McGraw-Hill