CISA Audit Exam Prep 2026

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1005 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/cisa
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1005 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play

Practice Questions

Try all 30 first, then check the answer key at the back.

1. In the COBIT framework for IT governance, what does the first principle of the framework focus on?

A. Covering the enterprise end-to-end
B. Applying a single integrated framework
C. Enabling a holistic approach
D. Meeting stakeholder needs

2. In a semiquantitative risk assessment, what is characteristic of the scoring system used?

A. Uses descriptive labels associated with numeric values
B. Depends on the annual loss expectancy (ALE)
C. Based solely on expert judgment
D. Requires precise probability calculations

3. What major governance issue is introduced with Bring Your Own Device (BYOD) policies?

A. Employees can bypass traditional IT controls by using personal devices.
B. Anyone can install unauthorized applications.
C. Confidential information is accessible without any authentication.
D. Tracking personal device usage is simple and straightforward.

4. An IT company that handles large volumes of customer data has established a Data Integrity team. The team ensures data consistency and accuracy by monitoring data input and output. They run periodic checks to confirm data integrity and ensure proper documentation. Based on this scenario, what could an auditor recommend for the Data Integrity team?

A. Regularly validate the accuracy and consistency of data during processing
B. Implement organization-wide best practices for data management following ISO 27001
C. Assist in the creation and storage of data
D. Provide training in data governance standards and practices

5. Which process involves a comprehensive overhaul of company IT infrastructure to streamline operations and boost efficiency?

A. IT Infrastructure Reengineering
B. Lean Management
C. Agile Methodology
D. DevOps

6. At what point in the systems development life cycle (SDLC) should a project be reviewed for scope creep to ensure cost and time management?

A. During the testing phase
B. During the requirements gathering phase
C. During the baselining phase
D. During the initial planning phase

7. An IS auditor needs to validate all the following when evaluating an ERP implementation EXCEPT:

A. That a comprehensive ERP implementation methodology is in place
B. That data migration integrity is maintained
C. That network performance metrics are being followed
D. That user requirements specifications were approved

8. A company has recently transitioned to a new inventory management system. What is one metric they can use to evaluate the effectiveness of this new system?

A. Number of items stocked per month
B. Total sales volume increase
C. Customer order fulfillment time
D. Reduction in inventory inaccuracies

9. An organization is transferring its financial records to a newly implemented accounting software. To confirm the success of the transfer, the team compares the number of entries in the new software with the old system. They also compare the total monetary amounts in both systems. In addition, checksums are calculated for specific fields in the old system to verify they match the checksums in the new software. What potential issue could the organization encounter?

A. The total monetary amounts should differ between the two systems
B. Transfer of monetary data should occur before other types of data
C. Checksums can vary based on how each system stores data
D. The new software will manage fewer entries than the old system

10. In the context of project management, how does the Gantt chart differ from the Work Breakdown Structure (WBS)?

A. Gantt charts outline resource dependencies, while WBS organizes team roles.
B. A Gantt chart visually represents the project schedule, while WBS breaks down the project's deliverables.
C. A Gantt chart is used for resource allocation, while WBS focuses on project cost estimation.
D. Gantt charts are used for risk management, while WBS manages project scope.

11. Which of the following roles ensures that software development processes comply with regulatory and compliance requirements to protect sensitive information?

A. Systems architect
B. Project manager
C. Database administrator
D. Compliance officer

12. What type of security solution is implemented to mitigate risks for enterprise laptops and desktops?

A. IPS
B. Endpoint Protection
C. SIEM
D. DLP

13. Which feature of a firewall helps to manage and control web traffic based on the content of the data packets?

A. IP Filtering
B. Packet Header Inspection
C. Deep Packet Inspection (DPI)
D. Port Filtering

14. An organization implements a cloud-based storage solution allowing employees to access their files from anywhere. What advantage does this setup provide, similar to benefits seen in a three-tier client-server architecture?

A. Centralized data management
B. Localized data storage
C. Distributed processing
D. Data redundancy

15. Public Key Infrastructure (PKI) is a framework for securing communications using pairs of cryptographic keys. In which environment is PKI primarily intended to be used?

A. Local standalone systems
B. Mainframe systems
C. Personal devices
D. Internet and network communication

16. An auditor is evaluating the cybersecurity measures of a company. They observe that the company uses multi-factor authentication (MFA) for remote access, employs encrypted communications for internal emails, regularly updates antivirus software, and restricts access to sensitive servers using biometric scanners. Based on this information, what should the auditor recommend?

A. Stop encrypting internal email communications
B. Cease updating antivirus software regularly
C. Implement logging and monitoring of biometric access
D. Disable multi-factor authentication for remote access

17. What is the practice of searching through trash bins to find sensitive information that has been discarded without proper destruction?

A. War driving
B. Dumpster diving
C. Traffic analysis
D. War chalking

18. An auditor is reviewing the organization's information access protocols. Data types are categorized as "highly sensitive," "sensitive," "internal," and "public." Which type only requires access controls during modification?

A. Public
B. Highly Sensitive
C. Sensitive
D. Internal

19. Firewalls are systems designed to prevent unauthorized access to or from a private network. What are the two basic kinds of firewalls?

A. Symmetric and asymmetric
B. Static and dynamic
C. Public and private
D. Packet-filtering and stateful inspection

20. A company needs to ensure database transaction integrity between two sites. The primary database logs every change and sends these logs to a secondary site in real-time. The primary site proceeds with the transaction only after it confirms the secondary site has received the logs. What type of method is being used to ensure transaction integrity?

A. Asynchronous replication
B. Data mirroring
C. Log shipping
D. Synchronous replication

21. In the context of business continuity planning, which of the following is NOT considered a key component of a disaster recovery plan?

A. Communication plans
B. Employee training programs
C. Data backup and recovery procedures
D. Emergency response teams

22. An effective incident response plan should include several key phases. These phases encompass all of the following EXCEPT:

A. Detection and analysis
B. Containment, eradication, and recovery
C. Annual financial audit
D. Preparation

23. A company is currently defining how their disaster recovery procedures should be detailed and how their systems will need to operate to ensure business continuity. In which phase of the business continuity planning lifecycle are they?

A. Design
B. Testing
C. Implementation
D. Evaluation

24. What is the term for the software that is implemented on servers and desktops to automatically gather and transmit log files to a central repository?

A. Virtual machines
B. Microservices
C. Agents
D. Containers

25. Which of the following is NOT a phase in the standard risk management process for an information system?

A. Monitoring risks
B. Implementing risk mitigation measures
C. Identifying risks
D. Assessing risks

26. In a corporate network environment, one of the key aspects an auditor should review is the network switch. What is the primary function of a network switch?

A. Monitors network traffic for anomalies
B. Sets a flag indicating the status of each transmitted packet
C. Routes data based on IP addresses
D. Provides communication linkage among different devices in the network

27. Which statement accurately describes an aspect of how a risk assessment process should be structured in an organization?

A. Only senior management should conduct the risk assessments.
B. Risk assessments should only be conducted during internal audits.
C. External auditors should be brought in for every assessment.
D. Clear criteria need to be established for evaluating risk levels.

28. An auditor evaluates the quality of an information system control using a sample with a confidence level of 90%. What is the sampling risk?

A. The average of all sample values
B. 10%
C. 5%
D. The total variation of all samples

29. An auditor is assessing the compliance of internal controls in a financial institution. They select a sample size with a 95% confidence coefficient. What can be inferred about the reliability of the sample in representing the population?

A. It has an insufficient degree of comfort.
B. It has a high degree of comfort.
C. It has a low degree of comfort.
D. It has a very high degree of comfort.

30. An IS auditor is investigating a company's network security protocols. They discover that manual updates to the firewall rules are subject to human error due to the complexity and volume of rules. This scenario pertains to which of the following?

A. Detection risk
B. Sampling risk
C. Control risk
D. Inherent risk

Answer Key & Explanations

1. D — Meeting stakeholder needs
Answer: Meeting stakeholder needs The first principle of the COBIT framework focuses on meeting stakeholder needs by balancing value, risk, and resources. Covering the enterprise end-to-end is the second principle. Applying a single integrated framework is the third principle and enabling a holistic approach is the fourth principle.

2. A — Uses descriptive labels associated with numeric values
Answer: Uses descriptive labels associated with numeric values In a semiquantitative risk assessment, the scoring system employs descriptive labels that are associated with numeric values. This method is useful when using purely quantitative or purely qualitative methods is not feasible. For instance, a qualitative descriptor like "medium" might be represented by the number three. The other options do not describe the characteristics of a semiquantitative scoring system.

3. A — Employees can bypass traditional IT controls by using personal devices.
Answer: Employees can bypass traditional IT controls by using personal devices. BYOD policies can significantly increase the flexibility and mobility of employees. However, they introduce governance issues because employees can access company data on personal devices, thus sidestepping traditional IT controls. An organization needs to maintain security for sensitive or critical information while ensuring all devices accessing the network are secure. Tracking and monitoring these devices can be challenging but is crucial for data protection.

4. A — Regularly validate the accuracy and consistency of data during processing
Answer: Regularly validate the accuracy and consistency of data during processing In addition to checking data input and output, validation can be carried out during data processing. This helps ensure that the processing is adhering to prescribed standards and can identify potential issues earlier in the workflow. Implementing best practices for data management following ISO 27001 is a function of data governance. The Data Integrity team should not be involved in the data creation and storage process but should focus on validating and ensuring data accuracy. Additionally, the Data Integrity team can offer training in data governance standards and practices.

5. A — IT Infrastructure Reengineering
Answer: IT Infrastructure Reengineering IT Infrastructure Reengineering focuses on a broader restructuring of IT processes and systems to improve overall efficiency and performance. It aims to streamline operations, enhance flexibility, and reduce costs across the organization. Lean Management optimizes processes to eliminate waste. Agile Methodology focuses on iterative software development. DevOps integrates development and operations for faster delivery cycles.

6. C — During the baselining phase
Answer: During the baselining phase The baselining phase, also known as the design freeze, marks the cutoff point for the project design. In this phase, everything is reviewed for time and cost requirements. Any proposed changes are evaluated for their associated risks. Baselining helps in reducing scope creep. At this

point, version numbers are typically introduced. The initial planning phase involves high-level project planning. Testing occurs during the development phase. The requirements gathering phase happens before the design is finalized.

7. C — That network performance metrics are being followed
Answer: That network performance metrics are being followed. Network performance metrics are relevant to IT infrastructure but are not directly relevant to an ERP implementation audit. The IS auditor needs to ensure approvals were obtained for user requirements, a comprehensive methodology is in place for ERP implementation, and data migration integrity is maintained. The IS auditor needs to ensure approvals were obtained for the user requirements specifications, a comprehensive ERP implementation methodology is in place, and data migration integrity is maintained.

8. D — Reduction in inventory inaccuracies
The reduction in inventory inaccuracies can be used as a metric for the effectiveness of a new inventory management system. If the new system is effective, there will be fewer inventory discrepancies. The number of items stocked per month is a metric of stock volume. Total sales volume increase is a metric of business growth. Customer order fulfillment time is a metric of customer service efficiency.

9. C — Checksums can vary based on how each system stores data
Answer: Checksums can vary based on how each system stores data Each system may store data differently, which can affect checksum calculations. For instance, one system may use spaces to pad fields, while another may use nulls, leading to different checksum results. Comparing entry counts can confirm the completeness of the transfer. Total monetary amounts help to ensure numerical fields match across systems. Transfer of different types of data does not necessarily need to follow a specific order.

10. B — A Gantt chart visually represents the project schedule, while WBS breaks down the project's deliverables.
A Gantt chart is a graphical tool that represents the project schedule, showing activities against time. It helps project managers track progress and manage time effectively. A Work Breakdown Structure (WBS), on the other hand, decomposes the project's deliverables into smaller, manageable components, making it easier to assign responsibilities and track deliverables.

11. D — Compliance officer
Answer: Compliance officer The compliance officer is responsible for ensuring that software development processes adhere to all regulatory and compliance requirements, thereby protecting sensitive information. A systems architect designs the overall system structure. A project manager oversees project execution but doesn't focus on compliance. A database administrator manages database-related tasks.

12. B — Endpoint Protection
Answer: Endpoint Protection Endpoint protection refers to a comprehensive security solution used to safeguard laptops, desktops, and other endpoints. It includes antivirus, anti-malware, and firewall features to protect against various types of threats. Security information and event management (SIEM) is a solution for aggregating logs to identify threats and intrusions. Data loss prevention (DLP) is used for preventing data exfiltration. An intrusion prevention system (IPS) is used to actively stop incidents.

13. C — Deep Packet Inspection (DPI)
Answer: Deep Packet Inspection (DPI) Deep Packet Inspection (DPI) is a network packet filtering technique that examines the data part (and possibly also the header) of a packet as it passes an inspection point. DPI is

used to detect intrusions, filter out unwanted content (such as malware), and manage network traffic efficiently. Port filtering restricts traffic based on port numbers. IP filtering blocks or allows traffic based on IP addresses. Packet header inspection only examines the header of data packets, not their content.

14. A — Centralized data management
Answer: Centralized data management In a cloud-based storage solution, data is maintained centrally on remote servers. This setup allows for central management and access to data from multiple locations, similar to how a three-tier client-server architecture centralizes processing and data storage on central servers. Localized data storage and distributed processing do not reflect the centralized management aspect. Data redundancy refers to duplicating data to improve reliability, not centralized access.

15. D — Internet and network communication
Answer: Internet and network communication Public Key Infrastructure (PKI) is designed to enable secure communication and authentication over internet and network systems. It uses pairs of cryptographic keys: a public key that can be shared widely and a private key that is kept secret. PKI supports various security services such as confidentiality, integrity, and non-repudiation. By establishing a framework of digital certificates and trusted certification authorities, PKI helps in validating the identity of parties involved in communications. This is essential for secure online transactions, protected emails, and virtual private networks (VPNs).

16. C — Implement logging and monitoring of biometric access
Answer: Implement logging and monitoring of biometric access While the company has robust cybersecurity measures in place such as MFA, encryption, regular antivirus updates, and biometric scanners, it should also ensure comprehensive logging and monitoring of biometric access. This will help in detecting and responding to potential breaches more effectively.

17. B — Dumpster diving
Answer: Dumpster diving Dumpster diving refers to the practice of searching through commercial or residential waste to find information that can be used for malicious purposes. This can include discarded confidential documents, old computers, or personal information. To prevent this, organizations should ensure that sensitive information is properly shredded or stored securely before disposal. Traffic analysis is used to monitor and examine network traffic. War chalking involves marking locations with wireless networks. War driving involves scanning for wireless networks while driving.

18. A — Public
Answer: Public Public data is accessible to everyone. However, access controls are required when updating this information. Highly sensitive, sensitive, and internal data demand stricter access controls compared to public data.

19. D — Packet-filtering and stateful inspection
Answer: Packet-filtering and stateful inspection Firewalls are classified mainly as packet-filtering and stateful inspection firewalls. Packet-filtering firewalls filter traffic based on pre-determined policies or rules set by the administrator. Stateful inspection firewalls, also known as dynamic packet filtering, monitor the state of active connections and make decisions based on the context of the traffic. This allows for more advanced filtering and better security than simple packet-filtering firewalls. By employing both types of firewalls, organizations can provide multilayered protection against unauthorized access while keeping network performance optimized.

20. D — Synchronous replication
Answer: Synchronous replication Synchronous replication ensures transaction integrity by replicating data in real-time to a secondary site and requiring confirmation from the secondary site before proceeding with the transaction at the primary site. Asynchronous replication, in contrast, sends data to the secondary site without waiting for confirmation. Data mirroring replicates data at frequent intervals but may not ensure real-time consistency. Log shipping involves periodically sending transaction logs to a secondary site, which does not guarantee immediate consistency.

21. B — Employee training programs
Answer: Employee training programs Employee training programs are important but are not typically a key component of the disaster recovery plan itself. Key components of a disaster recovery plan include data backup and recovery procedures, emergency response teams, and communication plans to ensure that critical business functions can be restored after a disaster.

22. C — Annual financial audit
Answer: Annual financial audit An effective incident response plan includes several key phases: preparation, detection and analysis, containment, eradication, and recovery. An annual financial audit is important for financial oversight but is not a component of an incident response plan. Preparation involves setting up and configuring an incident response capability. Detection and analysis determine if an incident has occurred and analyze its impact. Containment, eradication, and recovery aim to control the incident, eliminate the threat, and restore normal operations. The annual financial audit assesses financial practices and compliance but does not directly relate to handling information security incidents.

23. A — Design
Answer: Design In the business continuity planning lifecycle, the design phase is where specific details of disaster recovery procedures and the necessary system operations for ensuring business continuity are defined. The testing phase involves testing the disaster recovery plans. The implementation phase is when the plans are put into action. The evaluation phase is when the plans and processes are reviewed for effectiveness.

24. C — Agents
Answer: Agents Agents are small software components used to gather and transmit data, such as log files, to a central repository for processing and storage. They are essential for automating system monitoring and backup tasks. Containers are self-contained software environments that include all necessary dependencies. Virtual machines are virtualized instances of physical machines. Microservices are a way of designing software as a collection of smaller, loosely coupled services.

25. B — Implementing risk mitigation measures
Correct answer: Implementing risk mitigation measures The standard risk management process includes identifying risks, assessing risks, and monitoring risks. However, actually implementing risk mitigation measures is beyond the scope of the risk management process itself.

26. D — Provides communication linkage among different devices in the network
Answer: Provides communication linkage among different devices in the network. A network switch facilitates communication links between various devices within the network. The IS auditor needs to examine the security and functional performance of the switch, review the switch’s configuration settings, and assess any third-party audit reports regarding its operations. If such audits are not available, a physical inspection may be

necessary. The other choices do not accurately describe the function of a network switch.

27. D — Clear criteria need to be established for evaluating risk levels.
Clear criteria need to be established for evaluating risk levels in any risk assessment process. This ensures consistency and reliability in assessing potential risks. While risk assessments can involve various stakeholders, it is not essential for only senior management to conduct them, nor should they be confined to internal audits. It is also not always necessary to bring in external auditors for each assessment.

28. B — 10%
Answer: 10% The sampling risk is equal to 1 minus the confidence level. For a confidence level of 90%, the sampling risk is $$1 - 0.90$$, which is 0.10 (10%). The total variation of all samples refers to the measure of dispersion of the sample values, while the average of all sample values is the sample mean.

29. B — It has a high degree of comfort.
Answer: It has a high degree of comfort. The confidence coefficient is the probability that the characteristics of a sample are a true representation of the population. For a greater confidence coefficient, a larger sample size should be used. A 90-percent confidence coefficient is considered low. A 99-percent confidence coefficient is very high. Below 90 percent is an insufficient degree of comfort.

30. C — Control risk
Answer: Control risk Control risk relates to the risk that a material error exists that would not be prevented or detected within an appropriate time period by the system of internal controls. In this example, the control risk associated with manual updates to the firewall rules would be high due to the complexity and volume of rules. Detection risk is the risk that material errors or misstatements will not be detected by the auditor. Inherent risk is the risk that something will occur without considering implemented controls. Sampling risk is the risk that the sampling method will not detect issues.

Ready to pass?

Unlock the full CISA Audit Exam Prep 2026 bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/cisa

Also on iOS & Android — search your exam name on the App Store or Google Play