CISM Security Mgr Practice 202

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Practice Questions

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

1. The National Institute of Standards and Technology (NIST) defines three categories of risk mitigation strategies in incident management. They are:

A. Avoidance, Transference, and Recovery
B. Transference, Mitigation, and Detection
C. Mitigation, Detection, and Recovery
D. Avoidance, Transference, and Mitigation

2. An international bank is concerned that a cyber-attack could disrupt their primary trading network. They decide to set up an alternate trading site that can be operational immediately if such an attack occurs. Additionally, they want a tertiary site as a fallback option in case the secondary site is compromised. They have also specified that they want to reduce costs for this tertiary site. As the information security manager, what would you recommend for the tertiary site?

A. Reciprocal agreement
B. Mirror site
C. Cold site
D. Hot site

3. Who is typically responsible for ensuring the proper handling and documentation of events during a disaster recovery process?

A. Network Administrator
B. Disaster Recovery Coordinator
C. Chief Information Officer (CIO)
D. Board of Directors (BoD)

4. What is the MAIN difference between symmetric and asymmetric encryption?

A. The speed of data processing
B. The type of data it can encrypt
C. The type of keys used for encryption and decryption
D. The algorithm's complexity

5. What is the primary difference between event correlation and anomaly detection?

A. Event correlation identifies deviations from a standard behavior. Anomaly detection links multiple related events to identify potential security incidents.
B. Anomaly detection relies on predefined patterns and rules to identify incidents. Event correlation identifies deviations from normal behavior to find potential threats.
C. Event correlation relies on a predefined baseline and compares it to current behavior. Anomaly detection links multiple related events based on predefined rules.
D. Event correlation links multiple related events to identify potential security incidents. Anomaly detection identifies deviations from a standard behavior.

6. A financial brokerage firm is preparing for a major market event that is expected to significantly increase their network traffic. They are concerned about their primary internet connection failing during peak trading hours. To ensure they remain operational in the event of a failure, what solution could they implement to MINIMIZE downtime?

A. Cloud-based backup
B. Virtual Private Network (VPN)
C. Redundant internet connections
D. Network load balancing

7. In the Disaster Recovery Plan (DRP), there must be a section that ensures the availability of backup power supplies, communication devices, and essential software for continuity. What is this section typically called?

A. Logistics
B. Technical support team
C. Emergency coordination team
D. Recovery Point Objective (RPO)

8. What is the primary method for an information security manager to ensure that the organization's network configurations are secure and avoid unauthorized access?

A. Compliance with financial audits
B. CEO's confidence in IT team
C. Regular vulnerability assessments
D. Approval by legal department

9. Which of the following metrics is BEST to assess the effectiveness of a company's data loss prevention (DLP) strategy?

A. Employee security training completion rate
B. Reduction in data breaches
C. Number of phishing attempts
D. Firewall activity logs

10. After a data protection strategy has been created, what should happen NEXT?

A. Compliance monitoring
B. Internal audit
C. Executive approval
D. Vulnerability assessment

11. To ensure that an organization's cybersecurity measures are both effective and justified, it is ESSENTIAL to:

A. Perform a cost-benefit analysis for proposed cybersecurity measures
B. Align cybersecurity measures with competitor strategies
C. Assure senior management that the cybersecurity measures are the best
D. Ensure cybersecurity measures align with business expansion plans

12. A policy mandating regular security awareness training for employees falls under which type of security control?

A. Physical
B. Managerial
C. Technical
D. Operational

13. Who would be the MOST interested in a Key Performance Indicator (KPI) that tracks the completion of mandatory information security training by employees?

A. Human Resources (HR) Manager
B. Compliance Officer
C. Executive Management
D. Information Security Manager

14. A company plans to implement a remote work policy. The managers are concerned about the security of the information transmitted over various online communication tools. What measure is BEST to ensure the confidentiality of the transmitted data?

A. Anti-virus software
B. Restricting use of personal devices
C. End-to-end encryption
D. Virtual Private Network (VPN)

15. If a data center is managed by a third-party vendor but exclusively used by a single company, what type of hosting model is this?

A. Dedicated hosting
B. Shared hosting
C. Hybrid hosting
D. Community hosting

16. Which of the following is MOST likely to be an example of a key performance indicator (KPI) for assessing database performance?

A. Number of unauthorized access attempts
B. Detected malware incidents
C. Backup frequency
D. Average query response time

17. In an organization, if a security mechanism is used to monitor and log network traffic based on specific rules, this mechanism is known as a(n):

A. Digital Rights Management (DRM)
B. Intrusion Detection System (IDS)
C. Firewall
D. Intrusion Prevention System (IPS)

18. In the context of ensuring data integrity while outsourcing data storage, which deployment model provides the BEST guarantee?

A. Public cloud
B. Hybrid cloud
C. Community cloud
D. Private cloud

19. Offering a financial incentive to employees for reporting suspicious activities within a company could be considered a:

A. Corrective control
B. Countermeasure
C. Preventive control
D. Safeguard

20. Your organization plans to outsource the management of its IT infrastructure to a third-party Managed Service Provider (MSP). When is the BEST time to conduct a risk assessment?

A. Six months into the service
B. Immediately after service begins
C. On a continuous basis
D. Before signing the contract

21. Who within an organization is responsible for ensuring that data privacy regulations are adhered to within business processes?

A. Data Protection Officer (DPO)
B. Compliance officer
C. Chief Information Officer (CIO)
D. Chief Privacy Officer (CPO)

22. When designing an incident response plan, it is ESSENTIAL for the information security manager to:

A. Develop a robust training program for all IT staff
B. Conduct frequent penetration testing to find vulnerabilities
C. Create a comprehensive incident documentation process
D. Ensure that senior management supports the incident response plan

23. In the context of developing an incident response plan, what is the FIRST step a security manager should take?

A. Train the incident response team
B. Identify critical assets
C. Deploy incident response tools
D. Assess current security measures

24. In a large corporation that employs both a Chief Information Security Officer (CISO) and an information security manager, which responsibility is more likely to be assigned to the CISO rather than the information security manager?

A. Implementation of security controls
B. Monitoring compliance with security policies
C. Managing security incidents and responses
D. Development of an enterprise-wide security governance framework

25. In the context of incident response planning, what is another way to describe the concept of 'risk avoidance'?

A. Risk elimination
B. Risk mitigation
C. Risk transfer
D. Risk acceptance

26. In a healthcare organization, what is the first action the information security manager should take to establish a comprehensive patient data protection program?

A. Conduct quantitative and qualitative risk assessments
B. Establish a policy from senior management
C. Plan a meeting to determine resources
D. Initiate a project to implement controls

27. If a company wants to ensure that only authorized devices can access its wireless network, what type of control should it implement?

A. Wireless Access Control
B. Intrusion Detection System (IDS)
C. Virtual Local Area Network (VLAN)
D. Encryption

28. What type of threat is represented by an employee unintentionally sharing sensitive internal documents with an unauthorized third party?

A. Internal threat
B. External threat
C. Malicious insider
D. Script kiddie

29. Which of the following is NOT an appropriate use of qualitative risk assessments?

A. When quantifiable data is not available
B. When assessing aspects like reputation damage
C. For calculating the annual loss expectancy
D. As an initial step in a risk analysis process

30. When assessing new cybersecurity initiatives, determining the primary goals for these initiatives should use an iterative process based on:

A. A comprehensive vulnerability analysis compared to industry standards
B. Implementing controls aligned with historical threat data
C. Management's ability to align cybersecurity with corporate culture
D. An analysis of costs and an evaluation of acceptable risk levels

Answer Key & Explanations

1. D — Avoidance, Transference, and Mitigation
Answer: Avoidance, Transference, and Mitigation NIST defines the three categories of risk mitigation strategies as: Avoidance (eliminating the risk factor entirely through preventive measures) Transference (shifting the risk to a third party, typically through insurance or outsourcing) Mitigation (reducing the impact or likelihood of the risk through control measures)

2. C — Cold site
Answer: Cold site A cold site is an appropriate choice for a bank expecting to rely on an alternative site (in this scenario: the secondary site) and needing a cost-effective tertiary option. If an extreme cyber-attack compromises the primary trading network, they can fail over to the alternate site. Once functional in the secondary site, they can then provision the cold site to become operational as needed. A hot site is not suitable because it does not align with the cost-reduction requirement for the tertiary site. A reciprocal agreement, which involves resource sharing with another entity, typically doesn't fit the banking industry's critical and sensitive operations. A mirror site is expensive and already operational, making it impractical as a backup for the alternate site. However, a bank might find a mirror site suitable as a primary or secondary option due to its real-time capabilities.

3. B — Disaster Recovery Coordinator
Answer: Disaster Recovery Coordinator The Disaster Recovery Coordinator is responsible for ensuring that disaster recovery plans are executed properly and that all actions and events are documented accordingly. They oversee the disaster recovery process to minimize downtime and data loss. The CIO will oversee the broader security strategy while the Board of Directors are informed stakeholders, and the Network Administrator focuses on maintaining network functionality.

4. C — The type of keys used for encryption and decryption
Correct answer: The type of keys used for encryption and decryption In symmetric encryption, the same key is used for both encryption and decryption. In asymmetric encryption, a pair of related but different keys (public and private) is used for encryption and decryption. The complexity of the algorithm, speed, and type of data are not the primary differences. Symmetric encryption algorithms tend to be less complex and faster, whereas asymmetric encryption is more complex but provides better security for key exchange purposes.

5. D — Event correlation links multiple related events to identify potential security incidents. Anomaly detection identifies deviations from a standard behavior.
Answer: Event correlation links multiple related events to identify potential security incidents. Anomaly detection identifies deviations from a standard behavior. The primary difference between event correlation and anomaly detection is that event correlation links multiple related events based on predefined patterns or rules, while anomaly detection identifies deviations from normal behavior. Event correlation relies on finding relationships between different security events, potentially indicating an incident. Anomaly detection, on the other hand, looks for unusual behavior that deviates from established baselines, indicating potential unknown threats.

6. C — Redundant internet connections
Answer: Redundant internet connections Redundant internet connections provide a backup internet link to switch to if the primary connection fails, thus ensuring continued operation with minimal downtime. Network load balancing distributes traffic efficiently but does not directly address redundancy in case of a primary connection failure. Cloud-based backup focuses on data backup rather than maintaining continuous network connectivity. A VPN secures connections but does not provide redundancy or backup internet links.

7. A — Logistics
Answer: Logistics This is the logistics section of the DRP — it ensures that necessary resources such as backup power supplies, communication devices, and essential software are available for continuity. The technical support team handles hardware and software issues. The emergency coordination team organizes response actions during an emergency. The RPO determines the maximum tolerable period data might be lost due to a major incident.

8. C — Regular vulnerability assessments
Answer: Regular vulnerability assessments Regular vulnerability assessments help identify weaknesses in network configurations and ensure they are secure, thus preventing unauthorized access. Approval by the legal department is not related to network security. Compliance with financial audits ensures financial integrity, not network security. An IT team's capability cannot replace regular technical assessments for ensuring network security.

9. B — Reduction in data breaches
Answer: Reduction in data breaches Monitoring the reduction in data breaches is the most effective measure of a DLP strategy's success, as it directly correlates with the primary goal of preventing data loss. The other options, while useful for specific security aspects, do not directly measure the effectiveness of the overall DLP strategy.

10. C — Executive approval
Answer: Executive approval A data protection strategy should be reviewed and approved by the executive team before it can be put into action. A vulnerability assessment is needed prior to creating a protection strategy; once developed, a strategy should be executed following proper approval. Monitoring compliance happens after the strategy has been implemented. Internal audits can be carried out at any stage, but they typically follow the approval process.

11. A — Perform a cost-benefit analysis for proposed cybersecurity measures
Answer: Perform a cost-benefit analysis for proposed cybersecurity measures A cost-benefit analysis should be conducted for each of the proposed cybersecurity measures to confirm that the costs of implementing these measures are justified by the reduction in risk or impact. Aligning measures with competitor strategies or assuring management without hard data won't ensure effectiveness. Business expansion plans are indirectly related. A cost-benefit analysis directly ensures that the proposed measures are necessary and suitable.

12. B — Managerial
Answer: Managerial The policy is a managerial control. Training sessions themselves could be operational, while the content delivery might involve technical controls. However, the creation and enforcement of the policy is managerial.

13. D — Information Security Manager
Answer: Information Security Manager The information security manager is responsible for ensuring that all employees understand and comply with security policies. Therefore, they would be most interested in tracking the completion of mandatory training. Human Resources (HR) is likely concerned with the administrative aspects of enrolling employees in training but not specifically tracking security training completion. The compliance officer would be more interested in ensuring compliance with regulations but not to the same day-to-day extent as the information security manager. Executive management would be more concerned with the overall compliance and improvement but not the specific tracking of training completion.

14. C — End-to-end encryption
Answer: End-to-end encryption The best answer is end-to-end encryption, as it ensures that data transmitted over the internet remains confidential and cannot be intercepted by unauthorized parties. Using a VPN can provide some security but doesn't guarantee end-to-end encryption of data. Anti-virus software does not protect data transmitted over networks. Restricting the use of personal devices can limit potential security risks, but does not directly ensure the confidentiality of transmitted data.

15. A — Dedicated hosting
Answer: Dedicated hosting This is the definition of dedicated hosting. It can be managed by a third-party vendor but is used exclusively by a single company. The key is that the hosting environment is dedicated to this single customer. If the hosting environment is shared with others, it would be shared or community hosting. Shared hosting allows multiple companies to use the same servers without knowing about each other's presence. Community hosting enables multiple organizations with similar requirements to share the environment and possibly even the data. Hybrid hosting blends at least two of the hosting models: dedicated, shared, and community.

16. D — Average query response time
Answer: Average query response time Average query response time is an example of a key performance indicator (KPI). It measures the efficiency of database queries, indicating how quickly the database responds to requests. Number of unauthorized access attempts, detected malware incidents, and backup frequency are not KPIs directly related to database performance. While these metrics may be important for security and data protection, they do not measure the performance of database queries.

17. B — Intrusion Detection System (IDS)
Answer: Intrusion Detection System (IDS) An IDS is designed to monitor and log network traffic based on predefined rules and signatures. It does not actively block traffic but rather alerts the network administrator of any potentially malicious activity. In contrast, a firewall will block or allow traffic based on pre-configured rules, an IPS will block traffic based on a signature file or anomaly detection, and DRM controls access to digital content.

18. D — Private cloud
Answer: Private cloud To ensure data integrity while outsourcing data storage, the best solution is a private cloud. A private cloud has infrastructure dedicated exclusively to one customer, which minimizes the risk of data corruption or unauthorized access by other tenants. Public, hybrid, and community clouds involve multiple tenants from different organizations, which increases the complexity and risk associated with maintaining data integrity.

19. B — Countermeasure
Answer: Countermeasure A financial incentive for employees to report suspicious activities is a countermeasure. It is not a preventive control as it does not prevent the suspicious activity from occurring. Instead, it is a response aimed at identifying and addressing the activity after it has happened. A safeguard is a preventive control put in place to protect assets. A corrective control aims at fixing the issues after an incident has occurred. Here, the financial incentive does neither of these directly but acts as a response mechanism.

20. C — On a continuous basis
Answer: On a continuous basis A risk assessment should be conducted before signing any contract, but that is not enough. Risk assessments should be performed on a continuous basis to adapt to changing conditions and new potential risks. Although six months into the service and immediately after the service begins are important times, they are not the best. Continuous assessment ensures that any emerging risks are promptly identified and managed.

21. A — Data Protection Officer (DPO)
Answer: Data Protection Officer (DPO) The Data Protection Officer (DPO) is responsible for overseeing compliance with data privacy regulations within the organization. Compliance officers ensure that the company adheres to external regulations and internal policies, but they do not focus solely on data privacy. The CIO handles IT planning, budgeting, and performance. The Chief Privacy Officer (CPO) focuses on consumer data and privacy issues at a higher level within the organization.

22. D — Ensure that senior management supports the incident response plan
Answer: Ensure that senior management supports the incident response plan. Explanation: All answers detail important elements of incident response planning, but if senior management does not support the plan, it will be difficult to allocate the necessary resources. Senior management's support is critical for the effective implementation and continuous improvement of the incident response plan.

23. B — Identify critical assets
Answer: Identify critical assets Explanation: Before a security manager can develop an effective incident response plan, it is essential to identify and prioritize the organization’s critical assets. This ensures that the response plan focuses on protecting the most valuable and vulnerable parts of the infrastructure.

24. D — Development of an enterprise-wide security governance framework
Answer: Development of an enterprise-wide security governance framework A CISO is typically responsible for the strategic aspects of information security, which include the development of an enterprise-wide security governance framework. This role is more strategic and high-level compared to the tasks usually assigned to an information security manager, who focuses more on operational and tactical aspects, such as implementing controls, monitoring compliance, and managing incidents.

25. A — Risk elimination
Answer: Risk elimination Risk elimination is synonymous with risk avoidance. Risk mitigation, risk transfer, and risk acceptance are different concepts within risk management. Risk mitigation involves reducing the impact or likelihood of a risk. Risk transfer refers to shifting the risk to another party. Risk acceptance means acknowledging the risk and choosing not to address it.

26. B — Establish a policy from senior management
To build a successful patient data protection program, you must have management direction and support

documented within a policy regarding data protection. With a policy in place, you can proceed with planning and allocating resources, conducting risk assessments using various methodologies, and then initiating projects to implement appropriate controls.

27. A — Wireless Access Control
Answer: Wireless Access Control Wireless Access Control is used to ensure that only authorized devices can connect to a wireless network by verifying their credentials. An Intrusion Detection System (IDS) monitors network traffic for suspicious activity, but does not control access. A Virtual Local Area Network (VLAN) is used to partition a physical network into multiple, distinct segments. Encryption protects the confidentiality of data but does not control access to the network itself.

28. A — Internal threat
Answer: Internal threat An internal threat is anyone inside an organization that poses potential harm to the organization. This can happen without malicious intent, such as accidentally sharing sensitive information. An external threat originates from outside the organization, such as hackers or competitive entities. A malicious insider is an employee intentionally causing harm or leak of sensitive data. Script kiddies are amateur hackers using pre-written code without real understanding; they pose as external threats.

29. C — For calculating the annual loss expectancy
Answer: For calculating the annual loss expectancy Qualitative risk assessments are generally descriptive and do not provide hard numbers. They are suitable for: 1. Initial risk assessments to prioritize further analysis. 2. Situations where quantifiable data is unavailable. 3. Assessments for non-tangible aspects, such as reputation damage. Qualitative risk assessments should not be used for calculating specific values such as the annual loss expectancy, which requires quantitative data.

30. D — An analysis of costs and an evaluation of acceptable risk levels
Answer: An analysis of costs and an evaluation of acceptable risk levels The correct primary goals for cybersecurity initiatives must be established by evaluating the financial requirements to reach the target state and assessing whether the risk levels are within acceptable thresholds.

Ready to pass?

Unlock the full CISM Security Mgr Practice 202 bank, every explanation, and unlimited timed mock exams.

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

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