# The Best CISM Exam Study Material Premium Files and Preparation Tool (Apr-2025) [Q181-Q202


**The Best CISM Exam Study Material Premium Files and Preparation Tool (Apr-2025) Get Instant Access to CISM Practice Exam Questions**

ISACA CISM (Certified Information Security Manager) certification exam is designed for individuals who want to demonstrate their knowledge and expertise in information security management. Certified Information Security Manager certification exam is administered by the Information Systems Audit and Control Association (ISACA), which is a global association of professionals in the field of information technology governance, security, and assurance. The CISM certification exam is highly respected and recognized in the industry, and it is designed to evaluate an individual's ability to manage, design, and oversee an organization's information security program.

**QUESTION 181**

An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:
* risk assessment results.

* international security standards.
* the most stringent requirements.
* the security organization structure.

**QUESTION 182**

Which of the following is MOST important to include in an information security status report management?
* List of recent security events
* Key risk indication (KRIs)
* Review of information security policies
* information security budget requests

Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization’s objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004

**QUESTION 183**

An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?
* Right to audit
* Nondisclosure agreement
* Proper firewall implementation
* Dedicated security manager for monitoring compliance

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a business need to examine whether the controls are working effectively at the third party. Options B, C and D are important requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

**QUESTION 184**

Which of the following are likely to be updated MOST frequently?
* Procedures for hardening database servers
* Standards for password length and complexity
* Policies addressing information security governance
* Standards for document retention and destruction

Explanation

Policies and standards should generally be more static and less subject to frequent change. Procedures on the other hand, especially with regard to the hardening of operating systems, will be subject to constant change; as operating systems change and evolve, the procedures for hardening will have to keep pace.

**QUESTION 185**

Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?
* Patch management
* Change management
* Security metrics
* Version control
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT

Explanation:

Change management controls the process of introducing changes to systems. Failure to have good change management may introduce new weaknesses into otherwise secure systems. Patch management corrects discovered weaknesses by applying a correction to the original program code. Security metrics provide a means for measuring effectiveness. Version control is a subset of change management.

**QUESTION 186**

Which of the following is the PRIMARY objective of incident triage?
* Coordination of communications
* Mitigation of vulnerabilities
* Categorization of events
* Containment of threats
The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization’s information security.

Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization’s assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident.
Reference = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; Critical Incident Stress Management – National Interagency Fire Center3; Critical Incident Stress Management – US Forest Service4

**QUESTION 187**

When developing an asset classification program, which of the following steps should be completed FIRST?
* Categorize each asset.
* Create an inventory. &
* Create a business case for a digital rights management tool.
* Implement a data loss prevention (OLP) system.

**QUESTION 188**

Labeling information according to its security classification:
* enhances the likelihood of people handling information securely.
* reduces the number and type of countermeasures required.

* reduces the need to identify baseline controls for each classification.
* affects the consequences if information is handled insecurely.

Labeling information according to its security classification enhances the likelihood of people handling information securely. Security classification is a process of categoriz-ing information based on its level of sensitivity and importance, and applying appropri-ate security controls based on the level of risk associated with that infor-mation1. Labeling is a process of marking the information with the appropriate classifi-cation level, such as public, internal, confidential, secret, or top secret2. The purpose of labeling is to inform the users of the information about its value and protection re-quirements, and to guide them on how to handle it securely. Labeling can help users to:

* Identify the information they are dealing with and its classification level

* Understand their roles and responsibilities regarding the information

* Follow the security policies and procedures for the information

* Avoid unauthorized access, disclosure, modification, or destruction of the information

* Report any security incidents or breaches involving the information

Labeling can also help organizations to:

* Track and monitor the information and its usage

* Enforce access controls and encryption for the information

* Audit and review the compliance with security standards and regulations for the infor-mation

* Educate and train employees and stakeholders on information security awareness and best practices Therefore, labeling information according to its security classification enhances the likelihood of people handling information securely, as it increases their awareness and accountability, and supports the implementation of security measures. The other op-tions are not the primary benefits of labeling information according to its security clas-sification. Reducing the number and type of countermeasures required is not a benefit, but rather a consequence of applying security controls based on the classification lev-el. Reducing the need to identify baseline controls for each classification is not a bene-fit, but rather a prerequisite for labeling information according to its security classifica-tion. Affecting the consequences if information is handled insecurely is not a benefit, but rather a risk that needs to be managed by implementing appropriate security con-trols and incident response procedures. Reference: 1: Information Classification – Ad-visera 2: Information Classification in Information Security – GeeksforGeeks : Infor-mation Security Policy – NIST : Information Security Classification Framework – Queensland Government

**QUESTION 189**

An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

* Ethics
* Proportionality
* Integration
* Accountability

Explanation

Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information. It is advisable to learn if the job description is apportioning more data than are necessary for that position to execute the business rules

(types of data access). Principles of ethics and integration have the least to do with mapping job description to types of data access. The principle of accountability would be the second most adhered to principle since people with access to data may not always be accountable but may be required to perform an operation.

**QUESTION 190**

When aligning an organization’s information security program with other risk and control activities, it is MOST important to:
* develop an information security governance framework.
* have information security management report to the chief risk officer.
* ensure adequate financial resources are available.
* integrate security within the system development life cycle.

Section: INCIDENT MANAGEMENT AND RESPONSE

**QUESTION 191**

What should an information security team do FIRST when notified by the help desk that an employee’s computer has been infected with malware?
* Take a forensic copy of the hard drive.
* Restore the files from a secure backup.
* Isolate the computer from the network.
* Use anti-malware software to clean the infected computer.

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

**QUESTION 192**

During the selection of a Software as a Service (SaaS) vendor for a business process, the vendor provides evidence of a globally accepted information security certification. Which of the following is the MOST important consideration?
* The certification includes industry-recognized security controls.
* The certification was issued within the last five years.
* The certification is issued for the specific scope.
* The certification is easily verified.

The most important consideration when selecting a SaaS vendor for a business process is whether the vendor’ s information security certification is issued for the specific scope of the service that the organization needs. A certification that covers the entire vendor organization or a different service may not be relevant or sufficient for the organization’s security requirements. The certification should also include industry-recognized security controls, be issued within a reasonable time frame, and be easily verified, but these are not as critical as the scope.

References = CISM Review Manual, 16th Edition, page 1841; 5 Top SaaS Security Certifications for SaaS Providers

**QUESTION 193**

An enterprise has decided to procure security services from a third-party vendor to support its information security program. Which of the following is MOST important to include in the vendor selection criteria?
* Feedback from the vendor’s previous clients
* Alignment of the vendor’s business objectives with enterprise security goals
* The maturity of the vendor’s internal control environment
* Penetration testing against the vendor’s network

Explanation

The most important thing to include in the vendor selection criteria when procuring security services from a third-party vendor is B. Alignment of the vendor’s business objectives with enterprise security goals. This is because the vendor should be able to understand and support the enterprise’s security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. The vendor should also be able to demonstrate how their services add value, reduce risk, and enhance the performance and maturity of the enterprise’s information security program. The alignment of the vendor’s business objectives with enterprise security goals can help to ensure a successful and long-term partnership, and avoid any conflicts, gaps, or issues that may arise from misalignment or divergence.

The vendor should be able to understand and support the enterprise’s security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; Third-Party Vendor Selection: If Done Right, It’s a Win-Win2; Vendor Selection Criteria: Key Factors in Procurement Success3

**QUESTION 194**

When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:
* aligned with the IT strategic plan.
* based on the current rate of technological change.
* three-to-five years for both hardware and software.
* aligned with the business strategy.
Section: INFORMATION SECURITY GOVERNANCE

Explanation:

Any planning for information security should be properly aligned with the needs of the business. Technology should not come before the needs of the business, nor should planning be done on an artificial timetable that ignores business needs.

**QUESTION 195**

A global organization is developing an incident response team (IRT). The organization wants to keep headquarters informed of all incidents and wants to be able to present a unified response to widely dispersed events.

Which of the following IRT models BEST supports these objectives?
* Holistic IRT
* Central IRT
* Coordinating IRT
* Distributed IRT
Section: INCIDENT MANAGEMENT AND RESPONSE

**QUESTION 196**

An organization is considering the purchase of a competitor. To determine the competitor’s security posture, the BEST course of action for the organization’s information security manager would be to:
* assess the security policy of the competitor.
* assess the key technical controls of the competitor.
* conduct a penetration test of the competitor.
* perform a security gap analysis on the competitor.
Section: INFORMATION SECURITY PROGRAM MANAGEMENT

**QUESTION 197**

Which of the following is the GREATEST benefit of an information security architecture?
* Closer integration with the incident response team function
* Alignment with industry best practices
* Ease of integration between different security components
* Fewer false positives in the security incident and event management (SIEM)

**QUESTION 198**

A business requires a legacy version of an application to operate but the application cannot be patched. To limit the risk exposure to the business, a firewall is implemented in front of the legacy application. Which risk treatment option has been applied?
* Mitigate
* Accept
* Transfer
* Avoid

Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures.

A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched.

Therefore, mitigate is the correct answer.

References:

* https://simplicable.com/risk/risk-treatment

* https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

* https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm- process/risk-treatment.

**QUESTION 199**

A business unit recently integrated the organization’s new strong password policy into its business application which requires users to reset passwords every 30 days. The help desk is now flooded with password reset requests. Which of the following is the information security manager’s BEST course of action to address this situation?
* Provide end-user training.
* Escalate to senior management.
* Continue to enforce the policy.
* Conduct a business impact analysis (BIA).

**QUESTION 200**

A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?
* Escrow of software code with conditions for code release
* Right of the subscriber to conduct onsite audits of the vendor
* Authority of the subscriber to approve access to its data

* Commingling of subscribers’ data on the same physical server

**QUESTION 201**

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:
* results of exit interviews.
* previous training sessions.
* examples of help desk requests.
* responses to security questionnaires.

Explanation

The best way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include examples of help desk requests. Help desk requests are requests for assistance or support from users who encounter problems or issues related to information security, such as password resets, malware infections, phishing emails, unauthorized access, data loss, or system errors. Help desk requests can provide valuable insights into the types, frequencies, and impacts of the incidents that affect the users, as well as the users’ knowledge, skills, and behaviors regarding information security. By including examples of help desk requests in the user security awareness training program, the information security manager can achieve the following benefits12:

Increase the relevance and effectiveness of the training content: By using real-life scenarios and cases that the users have experienced or witnessed, the information security manager can make the training content more relevant, engaging, and applicable to the users’ needs and situations. The information security manager can also use the examples of help desk requests to illustrate the consequences and costs of the incidents, and to highlight the best practices and solutions to prevent or resolve them. This can help the users to understand the importance and value of information security, and to improve their knowledge, skills, and attitudes accordingly.

Identify and address the gaps and weaknesses in the training program: By analyzing the patterns and trends of the help desk requests, the information security manager can identify and address the gaps and weaknesses in the existing training program, such as outdated or inaccurate information, insufficient or ineffective coverage of topics, or lack of feedback or evaluation. The information security manager can also use the examples of help desk requests to measure and monitor the impact and outcomes of the training program, such as changes in the number, type, or severity of the incidents, or changes in the users’ satisfaction, performance, or behavior.

Enhance the communication and collaboration with the users and the help desk staff: By including examples of help desk requests in the user security awareness training program, the information security manager can enhance the communication and collaboration with the users and the help desk staff, who are the key stakeholders and partners in information security. The information security manager can use the examples of help desk requests to solicit feedback, suggestions, or questions from the users and the help desk staff, and to provide them with timely and relevant information, guidance, or support. The information security manager can also use the examples of help desk requests to recognize and appreciate the efforts and contributions of the users and the help desk staff in reporting, responding, or resolving the incidents, and to encourage and motivate them to continue their involvement and participation in information security.

The other options are not the best way to ensure that frequently encountered incidents are reflected in the user security awareness training program, as they are less reliable, relevant, or effective sources of information.

Results of exit interviews are feedback from employees who are leaving the organization, and they may not reflect the current or future incidents that the remaining or new employees may face. Previous training sessions are records of the past training activities, and they may not capture the changes or updates in the information security environment, threats, or requirements. Responses to security questionnaires are answers to predefined questions or surveys, and they may not cover all the possible or emerging incidents

that the users may encounter or experience12. References = Information Security Awareness Training: Best Practices – Infosec Resources, How to Create an Effective Security Awareness Training Program – Infosec Resources, Security Awareness Training: How to Build a Successful Program – ISACA, Security Awareness Training: How to Educate Your Employees – ISACA

**QUESTION 202**

Which of the following would a security manager establish to determine the target for restoration of normal processing?
* Recover time objective (RTO)
* Maximum tolerable outage (MTO)
* Recovery point objectives (RPOs)
* Services delivery objectives (SDOs)

Explanation

Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.