# Certified Information Security Manager

## Isaca CISM

Version Demo

Total Demo Questions: 15

Total Premium Questions: 258

## QUESTION NO: 1

Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

**A.** Including service level agreements (SLAs) in vendor contracts

**B.** Establishing communication paths with vendors

**C.** Requiring security awareness training for vendor staff

**D.** Performing integration testing with vendor systems

**ANSWER: B**

## QUESTION NO: 2

Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?

**A.** Regulations and standards

**B.** People and culture

**C.** Executive and board directives

**D.** Processes and technology

**ANSWER: B**

## QUESTION NO: 3

Which of the following should be the PRIMARY objective of an information security governance framework?

**A.** Provide a baseline for optimizing the security profile of the organization.

**B.** Demonstrate senior management commitment.

**C.** Demonstrate compliance with industry best practices to external stakeholders.

**D.** Ensure that users comply with the organization's information security policies.

**ANSWER: A**

**Explanation:**

According to the Certified Information Security Manager (CISM) Study Manual, "The primary objective of information security governance is to provide a framework for managing and controlling information security practices and technologies at an enterprise level. Its goal is to manage and reduce risk through a process of identification, assessment, and management of those risks."

While demonstrating senior management commitment, compliance with industry best practices, and ensuring user compliance with policies are all important aspects of information security governance, they are not the primary objective. The primary objective is to manage and reduce risk by establishing a framework for managing and controlling information security practices and technologies at an enterprise level.

Reference:

## QUESTION NO: 4

The PRIMARY objective of performing a post-incident review is to:

**A.** re-evaluate the impact of incidents.

**B.** identify vulnerabilities.

**C.** identify control improvements.

**D.** identify the root cause.

## ANSWER: D

**Explanation:**

The primary objective of performing a post-incident review is to identify the root cause of the incident. This information is used to develop and implement corrective actions to prevent similar incidents from occurring in the future. The post-incident review process may also include a re-evaluation of the impact of the incidents, the identification of vulnerabilities, and the identification of control improvements, but the primary objective is to determine the root cause of the incident. By understanding the root cause, the organization can take proactive steps to prevent similar incidents from occurring in the future and improve the overall security posture of the organization.

## QUESTION NO: 5

Which of the following is the BEST reason for an organization to use Disaster Recovery as a Service (DRaaS)?

**A.** It transfers the risk associated with recovery to a third party.

**B.** It lowers the annual cost to the business.

**C.** It eliminates the need to maintain offsite facilities.

**D.** It eliminates the need for the business to perform testing.

## ANSWER: B

## QUESTION NO: 6

Which of the following is an example of risk mitigation?

**A.** Purchasing insurance

**B.** Discontinuing the activity associated with the risk

**C.** Improving security controls

**D.** Performing a cost-benefit analysis

**ANSWER: C**

**Explanation:**

Risk mitigation refers to the processes and strategies that organizations use to reduce the likelihood or impact of potential risks. Improving security controls is a classic example of risk mitigation. By implementing or enhancing security controls, organizations can reduce the risk of security incidents or breaches, such as data theft or unauthorized access. For example, implementing strong passwords, regularly updating software and systems, and training employees on security best practices are all ways to improve security controls and mitigate risk. Other examples of risk mitigation include implementing disaster recovery and business continuity plans, conducting regular security assessments and audits, and purchasing insurance.

## QUESTION NO: 7

Which of the following metrics BEST measures the effectiveness of an organization's information security program?

**A.** Increase in risk assessments completed

**B.** Reduction in information security incidents

**C.** Return on information security investment

**D.** Number of information security business cases developed

**ANSWER: C**

## QUESTION NO: 8

Which of the following BEST enables the integration of information security governance into corporate governance?

**A.** Well-decumented information security policies and standards

**B.** An information security steering committee with business representation

**C.** Clear lines of authority across the organization

**D.** Senior management approval of the information security strategy

**ANSWER: B**

## QUESTION NO: 9

The MOST appropriate time to conduct a disaster recovery test would be after:

**A.** major business processes have been redesigned.

**B.** the business continuity plan (BCP) has been updated.

**C.** the security risk profile has been reviewed

**D.** noncompliance incidents have been filed.

**ANSWER: A**

## QUESTION NO: 10

Which of the following BEST determines the allocation of resources during a security incident response?

**A.** Senior management commitment

**B.** A business continuity plan (BCP)

**C.** An established escalation process

**D.** Defined levels of severity

**ANSWER: D**

**Explanation:**

Defined levels of severity is the best determinant of the allocation of resources during a security incident response. Having defined levels of severity allows organizations to plan for and allocate resources for each level of incident, depending on the severity of the incident. This ensures that the right resources are allocated in a timely manner and that incidents are addressed appropriately.

## QUESTION NO: 11

Which of the following is MOST helpful in determining an organization's current capacity to mitigate risks?

**A.** Capability maturity model

**B.** Vulnerability assessment

**C.** IT security risk and exposure

**D.** Business impact analysis (BIA)

**ANSWER: A**

## QUESTION NO: 12

An organization's main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?

**A.** The information security manager

**B.** The data owner

**C.** The application owner

**D.** The security engineer

**ANSWER: B**

## QUESTION NO: 13

Which of the following analyses will BEST identify the external influences to an organization's information security?

**A.** Business impact analysis (BIA)

**B.** Gap analysis

**C.** Threat analysis

**D.** Vulnerability analysis

**ANSWER: C**

**Explanation:**

Threat analysis is a process that is used to identify and assess the external influences or threats that could potentially affect an organization's information security. It is used to identify potential risks and develop strategies to mitigate or reduce those risks. Threat analysis involves analyzing the environment, identifying potential threats and their potential impacts, and then evaluating the organization's current security measures and developing strategies to address any deficiencies.

## QUESTION NO: 14

Which of the following would be the MOST effective way to present quarterly reports to the board on the status of the information security program?

**A.** A capability and maturity assessment

**B.** Detailed analysis of security program KPIs

**C.** An information security dashboard

**D.** An information security risk register

**ANSWER: C**

**Explanation:**

An information security dashboard is an effective way to present quarterly reports to the board on the status of the information security program. It allows the board to quickly view key metrics and trends at a glance and to drill down into more detailed information as needed. The dashboard should include metrics such as total incidents, patching compliance, vulnerability scanning results, and more. It should also include high-level overviews of the security program and its components, such as the security policy, security architecture, and security controls.

## QUESTION NO: 15

Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

**A.** Collect additional metrics.

**B.** Perform a cost-benefit analysis.

**C.** Submit funding request to senior management.

**D.** Begin due diligence on the outsourcing company.

**ANSWER: B**