# Isaca CISM Practice Questions

**Shared by Welch on 17-08-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

Which of the following is the MOST effective way to ensure information security policies are understood?

### Options:

A- Implement a whistle-blower program.
B- Provide regular security awareness training.
C- Include security responsibilities in job descriptions.
D- Document security procedures.

### Answer:

B

### Explanation:

Security awareness training is the most effective way to ensure information security policies are understood, as it educates employees on the purpose, content and importance of the policies, and how to comply with them. (From CISM Review Manual 15th Edition)

## Question 2

Question Type: MultipleChoice

After a ransomware incident an organization's systems were restored. Which of the following should be of MOST concern to the information security manager?

### Options:

A- The service level agreement (SLA) was not met.
B- The recovery time objective (RTO) was not met.
C- The root cause was not identified.
D- Notification to stakeholders was delayed.

## Answer:

C

## Explanation:

= After a ransomware incident, the most important concern for the information security manager is to identify the root cause of the incident and prevent it from happening again. The root cause analysis (RCA) is a systematic process of finding and eliminating the underlying factors that led to the incident, such as vulnerabilities, misconfigurations, human errors, or malicious actions. Without performing a RCA, the organization may not be able to address the root cause and may face the same or similar incidents in the future, which could result in more damage, costs, and reputational loss. Therefore, the information security manager should prioritize the RCA over other concerns, such as meeting the SLA, RTO, or notification requirements, which are important but secondary to the RCA.

Reference= CISM Review Manual 15th Edition, page 254-2551; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 4202

# Question 3

Question Type: MultipleChoice

Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

## Options:

A- Security policy
B- Risk management framework
C- Risk appetite
D- Security standards

## Answer:

C

## Explanation:

= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and

objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical.Reference= CISM Review Manual 15th Edition, page 29, page 31.

## Question 4

Question Type: MultipleChoice

Which of the following will BEST facilitate integrating the information security program into corporate governance?

### Options:

A- Documentation of the threat landscape
B- An up-to-date security strategy
C- A minimum security baseline
D- Documentation of residual risk

### Answer:

D

### Explanation:

Documentation of residual risk (D) best facilitates the integration of the information security program into corporate governance because it directly supports executive decision-making and accountability, which are core elements of governance in CISM. Corporate governance requires senior management and the board to understand, evaluate, and formally accept risk in alignment with business objectives and risk appetite. Residual risk documentation clearly communicates what risk remains after controls are applied and whether that risk is within acceptable tolerance.

While documentation of the threat landscape (A), an up-to-date security strategy (B), and a minimum security baseline (C) are all important program components, they primarily support operational security management, not governance integration. Governance focuses on oversight, transparency, and risk ownership, all of which are enabled when residual risk is documented, reported, and escalated appropriately.

CISM emphasizes that integrating security into corporate governance requires framing security

outcomes in business risk terms that executives can act upon. Residual risk documentation provides the mechanism for informed risk acceptance, prioritization of investments, and alignment with enterprise risk management.

ISACA CISM Review Manual, Information Security Governance --- risk reporting, residual risk, and governance integration

ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

## Question 5

Question Type: MultipleChoice

Implementing the principle of least privilege PRIMARILY requires the identification of:

### Options:

A- job duties
B- data owners
C- primary risk factors.
D- authentication controls

### Answer:

A

### Explanation:

Implementing the principle of least privilege primarily requires the identification of job duties. Job duties are the specific tasks and responsibilities that an individual performs as part of their role in the organization. By identifying the job duties, the organization can determine the minimum access privileges necessary for each individual to perform their assigned function, and nothing more. This helps to reduce the risk of unauthorized access, misuse, or compromise of information and resources.The principle of least privilege is a key security principle that states that every module (such as a user, a process, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose12.

The other options are not the primary factors that require identification for implementing the principle of least privilege. Data owners are the individuals or entities that have the authority and responsibility to define the classification, usage, and protection of data. Data owners may be involved in granting or revoking access privileges to data, but they are not the ones who identify the job duties of the data users. Primary risk factors are the sources or causes of

potential harm or loss to the organization. Primary risk factors may influence the level of access privileges granted to users, but they are not the ones who define the job duties of the users. Authentication controls are the mechanisms that verify the identity of users or systems before granting access to resources. Authentication controls may enforce the principle of least privilege, but they are not the ones who determine the job duties of the users.Reference=

Principle of least privilege

What Is the Principle of Least Privilege and Why is it Important?- F51

4

## Question 6

Question Type: MultipleChoice

Which of the following should be the GREATEST concern for an information security manager when an annual audit reveals the organization's business continuity plan (BCP) has not been reviewed or updated in more than a year?

### Options:

A- An outdated BCP may result in less efficient recovery if an actual incident occurs.
B- The organization may suffer reputational damage for not following industry best practices.
C- The audit finding may impact the overall risk rating of the organization.
D- The lack of updates to the BCP may result in noncompliance with internal policies.

### Answer:

A

### Explanation:

A BCP is a document that outlines the processes and procedures to maintain or resume critical business functions and minimize the impact of a disruption on the organization's objectives, customers, and stakeholders. A BCP should be reviewed and updated regularly to reflect the changes in the organization's environment, risks, resources, and requirements. An outdated BCP may result in less efficient recovery if an actual incident occurs, as it may not account for the current situation, dependencies, priorities, or recovery strategies. This may lead to increased downtime, losses, or damages for the organization.

Reference= CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity

and Disaster Recovery Plans

## Question 7

Question Type: MultipleChoice

A business impact analysis (BIA) BEST enables an organization to establish:

### Options:

A- Total cost of ownership (TCO).
B- Restoration priorities.
C- Annualized loss expectancy (ALE).
D- Recovery methods.

### Answer:

B

### Explanation:

A business impact analysis (BIA) best enables an organization to establish restoration priorities (B). In CISM, the primary purpose of a BIA is to identify critical business processes, assess the impact of disruptions over time, and determine which functions must be restored first to minimize business impact. Restoration priorities are derived from factors such as maximum tolerable downtime, recovery time objectives (RTOs), and recovery point objectives (RPOs), all of which are key BIA outputs.

Total cost of ownership (A) is a financial analysis concept unrelated to continuity planning. Annualized loss expectancy (C) is an output of quantitative risk analysis, not a BIA. Recovery methods (D) are defined after restoration priorities are established and are part of business continuity and disaster recovery planning. CISM emphasizes that the BIA provides the business-driven foundation upon which recovery strategies and methods are later selected.

By clearly defining restoration priorities, the BIA ensures that continuity planning aligns with business objectives, risk appetite, and operational resilience requirements.

ISACA CISM Review Manual, Information Security Program Development and Management --- Business Impact Analysis (BIA) purpose and outcomes

ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and

Management

## Question 8

Question Type: MultipleChoice

Which option best is MOST important when developing an information security strategy?

### Options:

A- Engage stakeholders.
B- Assign data ownership.
C- Determine information types.
D- Classify information assets.

### Answer:

A

### Explanation:

Engaging stakeholders is the most important step when developing an information security strategy, as it ensures that the strategy is aligned with the business objectives, risks, and needs of the organization. Stakeholders include senior management, business units, IT staff, customers, regulators, and other relevant parties who have an interest or influence on the information security of the organization. By engaging stakeholders, the information security manager can gain their support, input, feedback, and buy-in for the strategy, as well as identify and prioritize the security requirements, expectations, and challenges.

Reference= CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 1

## Question 9

Question Type: MultipleChoice

An organization is planning to open a new office in another country. Sensitive data will be routinely sent between the two offices. What should be the information security manager's FIRST course of action?

## Options:

A- Develop customized security training for employees at the new office
B- Encrypt the data for transfer to the head office based on security manager approval
C- Update privacy policies to include the other country's laws and regulations
D- Identify applicable regulatory requirements to establish security policies

## Answer:

D

## Explanation:

The first course of action is to identify applicable regulatory requirements (D). CISM governance requires understanding legal and regulatory obligations before defining policies, controls, or technical measures. Encryption (B), training (A), and policy updates (C) must be based on regulatory requirements to ensure compliance and avoid legal exposure. Jurisdictional risk assessment is foundational when operating across borders.