

Isaca

Exam CISM

Certified Information Security Manager

Version: 6.1

[Total Questions: 631]

Topic break down

Topic	No. of Questions
Topic 1: INFORMATION SECURITY GOVERNANCE	139
Topic 2: INFORMATION RISK MANAGEMENT	135
Topic 3: INFORMATION SECURITY PROGRAM DEVELOPMENT	114
Topic 4: INFORMATION SECURITY PROGRAM MANAGEMENT	156
Topic 5: INCIDENT MANAGEMENT AND RESPONSE	87

Topic 1, INFORMATION SECURITY GOVERNANCE**Question No : 1 - (Topic 1)**

From an information security manager perspective, what is the immediate benefit of clearly-defined roles and responsibilities?

- A. Enhanced policy compliance
- B. Improved procedure flows
- C. Segregation of duties
- D. Better accountability

Answer: D

Explanation:

Without well-defined roles and responsibilities, there cannot be accountability. Choice A is incorrect because policy compliance requires adequately defined accountability first and therefore is a byproduct. Choice B is incorrect because people can be assigned to execute procedures that are not well designed. Choice C is incorrect because segregation of duties is not automatic, and roles may still include conflicting duties.

Question No : 2 - (Topic 1)

Information security projects should be prioritized on the basis of:

- A. time required for implementation.
- B. impact on the organization.
- C. total cost for implementation.
- D. mix of resources required.

Answer: B

Explanation:

Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time, cost and resource issues should be subordinate to this objective.

Question No : 3 - (Topic 1)

Which of the following is an advantage of a centralized information security organizational structure?

- A. It is easier to promote security awareness.
- B. It is easier to manage and control.
- C. It is more responsive to business unit needs.
- D. It provides a faster turnaround for security requests.

Answer: B

Explanation:

It is easier to manage and control a centralized structure. Promoting security awareness is an advantage of decentralization. Decentralization allows you to use field security personnel as security missionaries or ambassadors to spread the security awareness message. Decentralized operations allow security administrators to be more responsive. Being close to the business allows decentralized security administrators to achieve a faster turnaround than that achieved in a centralized operation.

Question No : 4 - (Topic 1)

When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

- A. Compliance with international security standards.
- B. Use of a two-factor authentication system.
- C. Existence of an alternate hot site in case of business disruption.
- D. Compliance with the organization's information security requirements.

Answer: D

Explanation:

From a security standpoint, compliance with the organization's information security requirements is one of the most important topics that should be included in the contract with third-party service provider. The scope of implemented controls in any ISO 27001-compliant organization depends on the security requirements established by each organization. Requiring compliance only with this security standard does not guarantee that a service provider complies with the organization's security requirements. The requirement

to use a specific kind of control methodology is not usually stated in the contract with third-party service providers.

Question No : 5 - (Topic 1)

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?

- A. Ethics
- B. Proportionality
- C. Integration
- D. Accountability

Answer: B

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 No : 6 - (Topic 1)

Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

- A. Information security manager
- B. Chief operating officer (COO)
- C. Internal auditor
- D. Legal counsel

Answer: B

Explanation:

The chief operating officer (COO) is highly-placed within an organization and has the most knowledge of business operations and objectives. The chief internal auditor and chief legal counsel are appropriate members of such a steering group. However, sponsoring the creation of the steering committee should be initiated by someone versed in the strategy and direction of the business. Since a security manager is looking to this group for direction, they are not in the best position to oversee formation of this group.

Question No : 7 - (Topic 1)

Obtaining senior management support for establishing a warm site can BEST be accomplished by:

- A. establishing a periodic risk assessment.
- B. promoting regulatory requirements.
- C. developing a business case.
- D. developing effective metrics.

Answer: C**Explanation:**

Business case development, including a cost-benefit analysis, will be most persuasive to management. A risk assessment may be included in the business case, but by itself will not be as effective in gaining management support. Informing management of regulatory requirements may help gain support for initiatives, but given that more than half of all organizations are not in compliance with regulations, it is unlikely to be sufficient in many cases. Good metrics which provide assurance that initiatives are meeting organizational goals will also be useful, but are insufficient in gaining management support.

Question No : 8 - (Topic 1)

Which of the following is responsible for legal and regulatory liability?

- A. Chief security officer (CSO)

- B. Chief legal counsel (CLC)
- C. Board and senior management
- D. Information security steering group

Answer: C

Explanation:

The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

Question No : 9 - (Topic 1)

When an organization is implementing an information security governance program, its board of directors should be responsible for:

- A. drafting information security policies.
- B. reviewing training and awareness programs.
- C. setting the strategic direction of the program.
- D. auditing for compliance.

Answer: C

Explanation:

A board of directors should establish the strategic direction of the program to ensure that it is in sync with the company's vision and business goals. The board must incorporate the governance program into the overall corporate business strategy. Drafting information security policies is best fulfilled by someone such as a security manager with the expertise to bring balance, scope and focus to the policies. Reviewing training and awareness programs may best be handled by security management and training staff to ensure that the training is on point and follows best practices. Auditing for compliance is best left to the internal and external auditors to provide an objective review of the program and how it meets regulatory and statutory compliance.

Question No : 10 - (Topic 1)

Which of the following are likely to be updated MOST frequently?

- A. Procedures for hardening database servers
- B. Standards for password length and complexity
- C. Policies addressing information security governance
- D. Standards for document retention and destruction

Answer: A

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 No : 11 - (Topic 1)

What is the PRIMARY role of the information security manager in the process of information classification within an organization?

- A. Defining and ratifying the classification structure of information assets
- B. Deciding the classification levels applied to the organization's information assets
- C. Securing information assets in accordance with their classification
- D. Checking if information assets have been classified properly

Answer: A

Explanation:

Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

Question No : 12 - (Topic 1)

Which of the following is the BEST justification to convince management to invest in an information security program?

- A. Cost reduction
- B. Compliance with company policies
- C. Protection of business assets
- D. Increased business value

Answer: D

Explanation:

Investing in an information security program should increase business value and confidence. Cost reduction by itself is rarely the motivator for implementing an information security program. Compliance is secondary to business value. Increasing business value may include protection of business assets.

Question No : 13 - (Topic 1)

The cost of implementing a security control should not exceed the:

- A. annualized loss expectancy.
- B. cost of an incident.
- C. asset value.
- D. implementation opportunity costs.

Answer: C

Explanation:

The cost of implementing security controls should not exceed the worth of the asset. Annualized loss expectancy represents the losses that are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

Question No : 14 - (Topic 1)

Which of the following MOST commonly falls within the scope of an information security governance steering committee?

- A. Interviewing candidates for information security specialist positions
- B. Developing content for security awareness programs
- C. Prioritizing information security initiatives
- D. Approving access to critical financial systems

Answer: C

Explanation:

Prioritizing information security initiatives is the only appropriate item. The interviewing of specialists should be performed by the information security manager, while the developing of program content should be performed by the information security staff. Approving access to critical financial systems is the responsibility of individual system data owners.

Question No : 15 - (Topic 1)

Investments in information security technologies should be based on:

- A. vulnerability assessments.
- B. value analysis.
- C. business climate.
- D. audit recommendations.

Answer: B

Explanation:

Investments in security technologies should be based on a value analysis and a sound business case. Demonstrated value takes precedence over the current business climate because it is ever changing. Basing decisions on audit recommendations would be reactive in nature and might not address the key business needs comprehensively. Vulnerability assessments are useful, but they do not determine whether the cost is justified.

Question No : 16 - (Topic 1)