

The PRIMARY objective of a security steering group is to:

- A. ensure information security covers all business functions.
- B. ensure information security aligns with business goals.
- C. raise information security awareness across the organization.
- D. implement all decisions on security management across the organization.

Correct Answer: B

Explanation:

The security steering group comprises senior management of key business functions and has the primary objective to align the security strategy with the business direction. Option A is incorrect because all business areas may not be required to be covered by information security; but, if they do, the main purpose of the steering committee would be alignment more so than coverage. While raising awareness is important, this goal would not be carried out by the committee itself. The steering committee may delegate part of the decision making to the information security manager; however, if it retains this authority, it is not the primary' goal.

QUESTION 76

Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

- A. it implies compliance risks.
- B. short-term impact cannot be determined.
- C. it violates industry security practices.
- D. changes in the roles matrix cannot be detected.

Correct Answer: A

Explanation:

Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.

QUESTION 77

When developing an information security program, what is the MOST useful source of information for determining available resources?

- A. Proficiency test
- B. Job descriptions
- C. Organization chart
- D. Skills inventory

Correct Answer: D

Explanation:

A skills inventory would help identify- the available resources, any gaps and the training requirements for developing resources. Proficiency testing is useful but only with regard to specific technical skills. Job descriptions would not be as useful since they may be out of date or not sufficiently detailed. An organization chart would not provide the details necessary to determine the resources required for this activity.

QUESTION 78

[CISM Exam Dumps](#) **[CISM PDF Dumps](#) **[CISM VCE Dumps](#) **[CISM Q&As](#)******

<https://www.ensurepass.com/CISM.html>

Information security should be:

- A. focused on eliminating all risks.
- B. a balance between technical and business requirements.
- C. driven by regulatory requirements.
- D. defined by the board of directors.

Correct Answer: B

Explanation:

Information security should ensure that business objectives are met given available technical capabilities, resource constraints and compliance requirements. It is not practical or feasible to eliminate all risks. Regulatory requirements must be considered, but are inputs to the business considerations. The board of directors does not define information security, but provides direction in support of the business goals and objectives.

QUESTION 79

Information security governance is PRIMARILY driven by:

- A. technology constraints.
- B. regulatory requirements.
- C. litigation potential.
- D. business strategy.

Correct Answer: D

Explanation:

Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all important factors, but they are necessarily in line with the business strategy.

QUESTION 80

Which of the following should be the FIRST step in developing an information security plan?

- A. Perform a technical vulnerabilities assessment
- B. Analyze the current business strategy
- C. Perform a business impact analysis
- D. Assess the current levels of security awareness

Correct Answer: B

Explanation:

Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.

QUESTION 81

At what stage of the applications development process should the security department initially become involved?

- A. When requested
- B. At testing
- C. At programming
- D. At detail requirements

Correct Answer: D

Explanation:

Information security has to be integrated into the requirements of the application's design. It should also be part of the information security governance of the organization. The application owner may not make a timely request for security involvement. It is too late during systems testing, since the requirements have already been agreed upon. Code reviews are part of the final quality assurance process.

QUESTION 82

When an organization hires a new information security manager, which of the following goals should this individual pursue FIRST?

- A. Develop a security architecture
- B. Establish good communication with steering committee members
- C. Assemble an experienced staff
- D. Benchmark peer organizations

Correct Answer: B

Explanation:

New information security managers should seek to build rapport and establish lines of communication with senior management to enlist their support. Benchmarking peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly, developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

QUESTION 83

A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

- A. Representation by regional business leaders
- B. Composition of the board
- C. Cultures of the different countries
- D. IT security skills

Correct Answer: C

Explanation:

Culture has a significant impact on how information security will be implemented. Representation by regional business leaders may not have a major influence unless it concerns cultural issues. Composition of the board may not have a significant impact compared to cultural issues. IT security skills are not as key or high impact in designing a multinational information security program as would be cultural issues.

QUESTION 84

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.

Correct 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 85

Which of the following is the BEST reason to perform a business impact analysis (BIA)?

- A. To help determine the current state of risk
- B. To budget appropriately for needed controls
- C. To satisfy regulatory requirements
- D. To analyze the effect on the business

Correct Answer: A

Explanation:

The BIA is included as part of the process to determine the current state of risk and helps determine the acceptable levels of response from impacts and the current level of response, leading to a gap analysis. Budgeting appropriately may come as a result, but is not the reason to perform the analysis. Performing an analysis may satisfy regulatory requirements, but is not the reason to perform one. Analyzing the effect on the business is part of the process, but one must also determine the needs or acceptable effect or response.

QUESTION 86

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.

Correct 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 87

A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BEST approach of the information security manager?

- A. Acceptance of the business manager's decision on the risk to the corporation
- B. Acceptance of the information security manager's decision on the risk to the corporation
- C. Review of the assessment with executive management for final input
- D. A new risk assessment and BIA are needed to resolve the disagreement

Correct Answer: C

Explanation:

Executive management must be supportive of the process and fully understand and agree with the results since risk management decisions can often have a large financial impact and require major changes. Risk management means different things to different people, depending upon their role in the organization, so the input of executive management is important to the process.

QUESTION 88

Who should drive the risk analysis for an organization?

- A. Senior management
- B. Security manager
- C. Quality manager
- D. Legal department

Correct Answer: B

Explanation:

Although senior management should support and sponsor a risk analysis, the know-how and the management of the project will be with the security department. Quality management and the legal department will contribute to the project.

QUESTION 89

Which of the following is MOST appropriate for inclusion in an information security strategy?

- A. Business controls designated as key controls
- B. Security processes, methods, tools and techniques
- C. Firewall rule sets, network defaults and intrusion detection system (IDS) settings
- D. Budget estimates to acquire specific security tools

Correct Answer: B

Explanation:

A set of security objectives, processes, methods, tools and techniques together constitute a security strategy. Although IT and business governance are intertwined, business controls may not be included in a security strategy. Budgets will generally not be included in an information security strategy. Additionally, until information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and intrusion detection system (IDS) settings are technical details subject to periodic change, and are not appropriate content for a strategy document.

QUESTION 90

An organization's board of directors has learned of recent legislation requiring organizations within the industry to enact specific safeguards to protect confidential customer information. What actions should the board take next?

- A. Direct information security on what they need to do
- B. Research solutions to determine the proper solutions
- C. Require management to report on compliance
- D. Nothing; information security does not report to the board