

Organizational or business risk should always take precedence. Involving each organizational unit in information security and establishing metrics to measure success will be viewed favorably by senior management after the overall organizational risk is identified.

QUESTION 60

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

Correct 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 61

In implementing information security governance, the information security manager is PRIMARILY responsible for:

- A. developing the security strategy.
- B. reviewing the security strategy.
- C. communicating the security strategy.
- D. approving the security strategy

Correct Answer: A

Explanation:

The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners. Reviewing the security strategy is the responsibility of a steering committee. The information security manager is not necessarily responsible for communicating or approving the security strategy.

QUESTION 62

The MOST important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

- A. storage capacity and shelf life.
- B. regulatory and legal requirements.
- C. business strategy and direction.
- D. application systems and media.

Correct Answer: D

Explanation:

Long-term retention of business records may be severely impacted by changes in application systems and media. For example, data stored in nonstandard formats that can only be read and interpreted by previously decommissioned applications may be difficult, if not impossible, to recover. Business strategy and direction do not generally apply, nor do legal and regulatory requirements. Storage capacity and shelf life are important but secondary issues.

QUESTION 63

Who is responsible for ensuring that information is categorized and that specific protective

measures are taken?

- A. The security officer
- B. Senior management
- C. The end user
- D. The custodian

Correct Answer: B

Explanation:

Routine administration of all aspects of security is delegated, but top management must retain overall responsibility. The security officer supports and implements information security for senior management. The end user does not perform categorization. The custodian supports and implements information security measures as directed.

QUESTION 64

Which of the following is MOST important to understand when developing a meaningful information security strategy?

- A. Regulatory environment
- B. International security standards
- C. Organizational risks
- D. Organizational goals

Correct Answer: D

Explanation:

Alignment of security with business objectives requires an understanding of what an organization is trying to accomplish. The other choices are all elements that must be considered, but their importance is secondary and will vary depending on organizational goals.

QUESTION 65

Which of the following is MOST likely to be discretionary?

- A. Policies
- B. Procedures
- C. Guidelines
- D. Standards

Correct Answer: C

Explanation:

Policies define security goals and expectations for an organization. These are defined in more specific terms within standards and procedures. Standards establish what is to be done while procedures describe how it is to be done. Guidelines provide recommendations that business management must consider in developing practices within their areas of control; as such, they are discretionary.

QUESTION 66

Which of the following would help to change an organization's security culture?

- A. Develop procedures to enforce the information security policy

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

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

- B. Obtain strong management support
- C. Implement strict technical security controls
- D. Periodically audit compliance with the information security policy

Correct Answer: B

Explanation:

Management support and pressure will help to change an organization's culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditing is not effective in changing the culture of the company.

QUESTION 67

Which of the following is the MOST important information to include in an information security standard?

- A. Creation date
- B. Author name
- C. Initial draft approval date
- D. Last review date

Correct Answer: D

Explanation:

The last review date confirms the currency of the standard, affirming that management has reviewed the standard to assure that nothing in the environment has changed that would necessitate an update to the standard. The name of the author as well as the creation and draft dates are not that important.

QUESTION 68

Which of the following would be the MOST important goal of an information security governance program?

- A. Review of internal control mechanisms
- B. Effective involvement in business decision making
- C. Total elimination of risk factors
- D. Ensuring trust in data

Correct Answer: D

Explanation:

The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs when, in fact, just the opposite is true. Involvement in decision making is important only to ensure business data integrity so that data can be trusted.

QUESTION 69

An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees hood the IT

helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example of:

- A. conflicting security controls with organizational needs.
- B. strong protection of information resources.
- C. implementing appropriate controls to reduce risk.
- D. proving information security's protective abilities.

Correct Answer: A

Explanation:

The needs of the organization were not taken into account, so there is a conflict. This example is not strong protection, it is poorly configured. Implementing appropriate controls to reduce risk is not an appropriate control as it is being used. This does not prove the ability to protect, but proves the ability to interfere with business.

QUESTION 70

Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

- A. Update platform-level security settings
- B. Conduct disaster recovery test exercises
- C. Approve access to critical financial systems
- D. Develop an information security strategy paper

Correct Answer: D

Explanation:

Developing a strategy paper on information security would be the most appropriate. Approving access would be the job of the data owner. Updating platform-level security and conducting recovery test exercises would be less essential since these are administrative tasks.

QUESTION 71

In order to highlight to management the importance of network security, the security manager should FIRST:

- A. develop a security architecture.
- B. install a network intrusion detection system (NIDS) and prepare a list of attacks.
- C. develop a network security policy.
- D. conduct a risk assessment.

Correct Answer: D

Explanation:

A risk assessment would be most helpful to management in understanding at a very high level the threats, probabilities and existing controls. Developing a security architecture, installing a network intrusion detection system (NIDS) and preparing a list of attacks on the network and developing a network security policy would not be as effective in highlighting the importance to management and would follow only after performing a risk assessment.

QUESTION 72

To achieve effective strategic alignment of security initiatives, it is important that:

- A. Steering committee leadership be selected by rotation.
- B. Inputs be obtained and consensus achieved between the major organizational units.

- C. The business strategy be updated periodically.
- D. Procedures and standards be approved by all departmental heads.

Correct Answer: B

Explanation:

It is important to achieve consensus on risks and controls, and obtain inputs from various organizational entities since security needs to be aligned to the needs of the organization. Rotation of steering committee leadership does not help in achieving strategic alignment. Updating business strategy does not lead to strategic alignment of security initiatives. Procedures and standards need not be approved by all departmental heads

QUESTION 73

Reviewing which of the following would BEST ensure that security controls are effective?

- A. Risk assessment policies
- B. Return on security investment
- C. Security metrics
- D. User access rights

Correct Answer: C

Explanation:

Reviewing security metrics provides senior management a snapshot view and trends of an organization's security posture. Choice A is incorrect because reviewing risk assessment policies would not ensure that the controls are actually working. Choice B is incorrect because reviewing returns on security investments provides business justifications in implementing controls, but does not measure effectiveness of the control itself. Choice D is incorrect because reviewing user access rights is a joint responsibility of the data custodian and the data owner, and does not measure control effectiveness.

QUESTION 74

Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

- A. Continuous analysis, monitoring and feedback
- B. Continuous monitoring of the return on security investment (ROSD)
- C. Continuous risk reduction
- D. Key risk indicator (KRD setup to security management processes)

Correct Answer: A

Explanation:

To improve the governance framework and achieve a higher level of maturity, an organization needs to conduct continuous analysis, monitoring and feedback compared to the current state of maturity. Return on security investment (ROSD) may show the performance result of the security-related activities; however, the result is interpreted in terms of money and extends to multiple facets of security initiatives. Thus, it may not be an adequate option. Continuous risk reduction would demonstrate the effectiveness of the security governance framework, but does not indicate a higher level of maturity. Key risk indicator (KRD setup is a tool to be used in internal control assessment. KRI setup presents a threshold to alert management when controls are being compromised in business processes. This is a control tool rather than a maturity model support tool.

QUESTION 75

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

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