

Correct Answer: B

Explanation:

The job of the information security officer on such a team is to assess the risks to the business operation. Choice A is incorrect because information security is not limited to IT issues. Choice C is incorrect because at the time a team is formed to assess risk, it is premature to assume that any demonstration of IT controls will mitigate business operations risk. Choice D is incorrect because it is premature at the time of the formation of the team to assume that any suggestion of new IT controls will mitigate business operational risk.

QUESTION 29

Who should be responsible for enforcing access rights to application data?

- A. Data owners
- B. Business process owners
- C. The security steering committee
- D. Security administrators

Correct Answer: D

Explanation:

As custodians, security administrators are responsible for enforcing access rights to data. Data owners are responsible for approving these access rights. Business process owners are sometimes the data owners as well, and would not be responsible for enforcement. The security steering committee would not be responsible for enforcement.

QUESTION 30

The FIRST step to create an internal culture that focuses on information security is to:

- A. implement stronger controls.
- B. conduct periodic awareness training.
- C. actively monitor operations.
- D. gain the endorsement of executive management.

Correct Answer: D

Explanation:

Endorsement of executive management in the form of policies provides direction and awareness. The implementation of stronger controls may lead to circumvention. Awareness training is important, but must be based on policies. Actively monitoring operations will not affect culture at all levels.

QUESTION 31

Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

- A. Obtain the support of the board of directors.
- B. Improve the content of the information security awareness program.
- C. Improve the employees' knowledge of security policies.
- D. Implement logical access controls to the information systems.

Correct Answer: A

Explanation:

It is extremely difficult to implement an information security program without the aid and support of the board of directors. If they do not understand the importance of security to the achievement of the business objectives, other measures will not be sufficient. Options B and (are measures proposed to ensure the efficiency of the information security program implementation, but are of less significance than obtaining the aid and support of the board of directors. Option D is a measure to secure the enterprise information, but by itself is not a measure to ensure the broader effectiveness of an information security program.

QUESTION 32

Which of the following would be MOST effective in successfully implementing restrictive password policies?

- A. Regular password audits
- B. Single sign-on system
- C. Security awareness program
- D. Penalties for noncompliance

Correct Answer: C

Explanation:

To be successful in implementing restrictive password policies, it is necessary to obtain the buy-in of the end users. The best way to accomplish this is through a security awareness program. Regular password audits and penalties for noncompliance would not be as effective on their own; people would go around them unless forced by the system. Single sign-on is a technology solution that would enforce password complexity but would not promote user compliance. For the effort to be more effective, user buy-in is important.

QUESTION 33

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

Correct 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 34

Acceptable levels of information security risk should be determined by:

- A. legal counsel.
- B. security management.
- C. external auditors.
- D. the steering committee.

Correct Answer: D

Explanation:

Senior management, represented in the steering committee, has ultimate responsibility for

determining what levels of risk the organization is willing to assume. Legal counsel, the external auditors and security management are not in a position to make such a decision.

QUESTION 35

Logging is an example of which type of defense against systems compromise?

- A. Containment
- B. Detection
- C. Reaction
- D. Recovery

Correct Answer: B

Explanation:

Detection defenses include logging as well as monitoring, measuring, auditing, detecting viruses and intrusion. Examples of containment defenses are awareness, training and physical security defenses. Examples of reaction defenses are incident response, policy and procedure change, and control enhancement. Examples of recovery defenses are backups and restorations, failover and remote sites, and business continuity plans and disaster recovery plans.

QUESTION 36

Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

- A. Key control monitoring
- B. A robust security awareness program
- C. A security program that enables business activities
- D. An effective security architecture

Correct Answer: C

Explanation:

A security program enabling business activities would be most helpful to achieve alignment between information security and organization objectives. All of the other choices are part of the security program and would not individually and directly help as much as the security program.

QUESTION 37

The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

- A. escalate issues to an external third party for resolution.
- B. ensure that senior management provides authority for security to address the issues.
- C. insist that managers or units not in agreement with the security solution accept the risk.
- D. refer the issues to senior management along with any security recommendations.

Correct Answer: D

Explanation:

Senior management is in the best position to arbitrate since they will look at the overall needs of the business in reaching a decision. The authority may be delegated to others by senior management after their review of the issues and security recommendations. Units should not be asked to accept the risk without first receiving input from senior management.

QUESTION 38

The FIRST step in developing an information security management program is to:

- A. identify business risks that affect the organization.
- B. clarify organizational purpose for creating the program.
- C. assign responsibility for the program.
- D. assess adequacy of controls to mitigate business risks.

Correct Answer: B

Explanation:

In developing an information security management program, the first step is to clarify the organization's purpose for creating the program. This is a business decision based more on judgment than on any specific quantitative measures. After clarifying the purpose, the other choices are assigned and acted upon.

QUESTION 39

What is the MOST important factor in the successful implementation of an enterprise wide information security program?

- A. Realistic budget estimates
- B. Security awareness
- C. Support of senior management
- D. Recalculation of the work factor

Correct Answer: C

Explanation:

Without the support of senior management, an information security program has little chance of survival. A company's leadership group, more than any other group, will more successfully drive the program. Their authoritative position in the company is a key factor. Budget approval, resource commitments, and companywide participation also require the buy-in from senior management. Senior management is responsible for providing an adequate budget and the necessary resources. Security awareness is important, but not the most important factor. Recalculation of the work factor is a part of risk management.

QUESTION 40

While implementing information security governance an organization should FIRST:

- A. adopt security standards.
- B. determine security baselines.
- C. define the security strategy.
- D. establish security policies.

Correct Answer: C

Explanation:

The first step in implementing information security governance is to define the security strategy based on which security baselines are determined. Adopting suitable security- standards, performing risk assessment and implementing security policy are steps that follow the definition of the security strategy.

QUESTION 41

Which of the following is MOST important in developing a security strategy?

- A. Creating a positive business security environment
- B. Understanding key business objectives
- C. Having a reporting line to senior management
- D. Allocating sufficient resources to information security

Correct Answer: B

Explanation:

Alignment with business strategy is of utmost importance. Understanding business objectives is critical in determining the security needs of the organization.

QUESTION 42

Which of the following roles would represent a conflict of interest for an information security manager?

- A. Evaluation of third parties requesting connectivity
- B. Assessment of the adequacy of disaster recovery plans
- C. Final approval of information security policies
- D. Monitoring adherence to physical security controls

Correct Answer: C

Explanation:

Since management is ultimately responsible for information security, it should approve information security policy statements; the information security manager should not have final approval. Evaluation of third parties requesting access, assessment of disaster recovery plans and monitoring of compliance with physical security controls are acceptable practices and do not present any conflicts of interest.

QUESTION 43

What would be the MOST significant security risks when using wireless local area network (LAN) technology?

- A. Man-in-the-middle attack
- B. Spoofing of data packets
- C. Rogue access point
- D. Session hijacking

Correct Answer: C

Explanation:

A rogue access point masquerades as a legitimate access point. The risk is that legitimate users may connect through this access point and have their traffic monitored. All other choices are not dependent on the use of a wireless local area network (LAN) technology.

QUESTION 44

Retention of business records should PRIMARILY be based on:

- A. business strategy and direction.
- B. regulatory and legal requirements.
- C. storage capacity and longevity.
- D. business ease and value analysis.

Correct Answer: B

Explanation:

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

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