Vendor: Isaca

Exam Code: CISM

Exam Name: Certified Information Security Manager

Version: DEMO

QUESTION 1
Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

A. organizational risk.
B. organization wide metrics.
C. security needs.
D. the responsibilities of organizational units.

Answer: A
Explanation:
Information security exists to help the organization meet its objectives. The information security manager should identify information security needs based on organizational needs. 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 2
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

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 3
Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

A. The information security department has difficulty filling vacancies.
B. The chief information officer (CIO) approves security policy changes.
C. The information security oversight committee only meets quarterly.
D. The data center manager has final signoff on all security projects.

Answer: D
Explanation:
A steering committee should be in place to approve all security projects. The fact that the data center manager has final signoff for all security projects indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This would indicate a failure of information security governance. It is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it may be desirable to have the chief information officer (CIO) approve the security policy due to the size of the organization and frequency of updates. Difficulty in filling vacancies is not uncommon due to the shortage of good,

qualified information security professionals.

QUESTION 4
Which of the following requirements would have the lowest level of priority in information security?

A. Technical
B. Regulatory
C. Privacy
D. Business

Answer: A
Explanation:
Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

QUESTION 5
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

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 6
It is MOST important that information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

Answer: D
Explanation:
Information security architecture should always be properly aligned with business goals and objectives. Alignment with IT plans or industry and security best practices is secondary by comparison.

QUESTION 7

Which of the following is MOST likely to be discretionary?

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

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 8
Security technologies should be selected PRIMARILY on the basis of their:

A. ability to mitigate business risks.
B. evaluations in trade publications.
C. use of new and emerging technologies.
D. benefits in comparison to their costs.

Answer: A
Explanation:
The most fundamental evaluation criterion for the appropriate selection of any security technology is its ability to reduce or eliminate business risks. Investments in security technologies should be based on their overall value in relation to their cost; the value can be demonstrated in terms of risk mitigation. This should take precedence over whether they use new or exotic technologies or how they are evaluated in trade publications.

QUESTION 9
Which of the following are seldom changed in response to technological changes?

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

Answer: C
Explanation:
Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change. Security standards and procedures as well as guidelines must be revised and updated based on the impact of technology changes.

QUESTION 10
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.

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 11
Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

A. More uniformity in quality of service
B. Better adherence to policies
C. Better alignment to business unit needs
D. More savings in total operating costs

Answer: C
Explanation:
Decentralization of information security management generally results in better alignment to business unit needs. It is generally more expensive to administer due to the lack of economies of scale. Uniformity in quality of service tends to vary from unit to unit.

QUESTION 12
Which of the following is the MOST appropriate position to sponsor the design and implementation of a new security infrastructure in a large global enterprise?

A. Chief security officer (CSO)
B. Chief operating officer (COO)
C. Chief privacy officer (CPO)
D. Chief legal counsel (CLC)

Answer: B
Explanation:
The chief operating officer (COO) is most knowledgeable of business operations and objectives. The chief privacy officer (CPO) and the chief legal counsel (CLC) may not have the knowledge of the day- to-day business operations to ensure proper guidance, although they have the same influence within the organization as the COO. Although the chief security officer (CSO) is knowledgeable of what is needed, the sponsor for this task should be someone with far-reaching influence across the organization.