Vendor: Isaca

Exam Code: CISM

Exam Name: Certified Information Security Manager

Version: Demo

QUESTION 1
When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

A. aligned with the IT strategic plan.
B. based on the current rate of technological change.
C. three-to-five years for both hardware and software.
D. aligned with the business strategy.

Correct Answer: D
Explanation:
Any planning for information security should be properly aligned with the needs of the business. Technology should not come before the needs of the business, nor should planning be done on an artificial timetable that ignores business needs.

QUESTION 2
A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

A. meet with stakeholders to decide how to comply.
B. analyze key risks in the compliance process.
C. assess whether existing controls meet the regulation.
D. update the existing security/privacy policy.

Correct Answer: C
Explanation:
If the organization is in compliance through existing controls, the need to perform other work related to the regulation is not a priority. The other choices are appropriate and important; however, they are actions that are subsequent and will depend on whether there is an existing control gap.

QUESTION 3
Which of the following represents the MAJOR focus of privacy regulations?

A. Unrestricted data mining
B. Identity theft
C. Human rights protection D.
D. Identifiable personal data

Correct Answer: D
Explanation:
Protection of identifiable personal data is the major focus of recent privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Data mining is an accepted tool for ad hoc reporting; it could pose a threat to privacy only if it violates regulator)' provisions. Identity theft is a potential consequence of privacy violations but not the main focus of many regulations. Human rights addresses privacy issues but is not the main focus of regulations.

QUESTION 4

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.

Correct 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 ease, 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 5
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.

Correct 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 6
The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

A. generally accepted industry best practices.
B. business requirements.
C. legislative and regulatory requirements.
D. storage availability.

Correct Answer: B
Explanation:
The primary concern will be to comply with legislation and regulation but only if this is a genuine business requirement. Best practices may be a useful guide but not a primary concern. Legislative and regulatory requirements are only relevant if compliance is a business need. Storage is irrelevant since whatever is needed must be provided

QUESTION 7
Senior management commitment and support for information security can BEST be enhanced

through:

A. a formal security policy sponsored by the chief executive officer (CEO).
B. regular security awareness training for employees.
C. periodic review of alignment with business management goals.
D. senior management signoff on the information security strategy.

Correct Answer: C
Explanation:
Ensuring that security activities continue to be aligned and support business goals is critical to obtaining their support. Although having the chief executive officer (CEO) signoff on the security policy and senior management signoff on the security strategy makes for good visibility and demonstrates good tone at the top, it is a one-time discrete event that may be quickly forgotten by senior management. Security awareness training for employees will not have as much effect on senior management commitment.

QUESTION 8
When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

A. Business management
B. Operations manager
C. Information security manager
D. System users

Correct Answer: C
Explanation:
The escalation process in critical situations should involve the information security manager as the first contact so that appropriate escalation steps are invoked as necessary. Choices A, B and D would be notified accordingly.

QUESTION 9
The MOST appropriate role for senior management in supporting information security is the:

A. evaluation of vendors offering security products.
B. assessment of risks to the organization.
C. approval of policy statements and funding.
D. monitoring adherence to regulatory requirements.

Correct Answer: C
Explanation:
Since the members of senior management are ultimately responsible for information security, they are the ultimate decision makers in terms of governance and direction. They are responsible for approval of major policy statements and requests to fund the information security practice. Evaluation of vendors, assessment of risks and monitoring compliance with regulatory requirements are day-to-day responsibilities of the information security manager; in some organizations, business management is involved in these other activities, though their primary role is direction and governance.

QUESTION 10
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
B. establish baseline standards for all locations and add supplemental standards as required.
C. bring all locations into conformity with a generally accepted set of industry best practices.
D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

Correct Answer: B
Explanation:
It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach--forcing all locations to be in compliance with the regulations places an undue burden on those locations.

QUESTION 11
Which of the following requirements would have the lowest level of priority in information security?

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

Correct 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 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)

Correct 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.
QUESTION 13
Information security projects should be prioritized on the basis of:

A. time required for implementation.