Demo Questions

ISACA CISM Exam

Certified Information Security Manager

Thank you for downloading **CISM** Exam PDF

Question #1 ***Topic 1***

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*
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 #2 ***Topic 1***

Senior management commitment and support for information security can BEST be obtained through presentations that:

- A. use illustrative examples of successful attacks.

- B. explain the technical risks to the organization.
- C. evaluate the organization against best security practices.
- D. tie security risks to key business objectives.

Correct Answer: *D*
Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives. Senior management will not be as interested in technical risks or examples of successful attacks if they are not tied to the impact on business environment and objectives. Industry best practices are important to senior management but, again, senior management will give them the right level of importance when they are presented in terms of key business objectives.

Question #3*Topic 1*

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*
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 #4*Topic 1*

Which of the following would BEST ensure the success of information security governance within an organization?

- A. Steering committees approve security projects
- B. Security policy training provided to all managers
- C. Security training available to all employees on the intranet
- D. Steering committees enforce compliance with laws and regulations

Correct Answer: *A*
The existence of a steering committee that approves all security projects would be an indication of the existence of a good governance program. Compliance with laws and regulations is part of the responsibility of the steering committee but it is not a full answer. Awareness training is important at all levels in any medium, and also an indicator of good governance. However, it must be guided and approved as a security project by the steering committee.

Question #5*Topic 1*

Information security governance is PRIMARILY driven by:

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

Correct Answer: *D*
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 #6*Topic 1*

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*
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 #7*Topic 1*

Investments in information security technologies should be based on:

- A. vulnerability assessments.
- B. value analysis.
- C. business climate.
- D. audit recommendations.

Correct Answer: *B*
Investments in security technologies should be based on a value analysis and a sound business case. Demonstrated value takes precedence over the current business climate because it is ever changing. Basing decisions on audit recommendations would be reactive in nature and might not address the key business needs comprehensively. Vulnerability assessments are useful, but they do not determine whether the cost is justified.

Question #8*Topic 1*

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*
Retention of business records is generally driven by legal and regulatory requirements. Business strategy and direction would not normally apply nor would they override legal and regulatory requirements. Storage capacity and longevity are important but secondary issues. Business case and value analysis would be secondary to complying with legal and regulatory requirements.

Question #9*Topic 1*

Which of the following is characteristic of centralized information security management?

- A. More expensive to administer
- B. Better adherence to policies
- C. More aligned with business unit needs
- D. Faster turnaround of requests

Correct Answer: *B*
Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to

the economics of scale. However, turnaround can be slower due to the lack of alignment with business units.

Question #10_Topic 1_

Successful implementation of information security governance will FIRST require:

- A. security awareness training.
- [✓ B. updated security policies.]
- C. a computer incident management team.
- D. a security architecture.

Correct Answer: *B*
Updated security policies are required to align management objectives with security procedures; management objectives translate into policy; policy translates into procedures. Security procedures will necessitate specialized teams such as the computer incident response and management group as well as specialized tools such as the security mechanisms that comprise the security architecture. Security awareness will promote the policies, procedures and appropriate use of the security mechanisms.