



CISM

(Certified Information Security Manager)

Document version: 6.28.11

Important Note About CISM PDF

techeXams' **CISM PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

techeXams holds the copyright of this material. techeXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Question: 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

Answer: B

Explanation:

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

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.

Answer: D

Explanation:

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

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.

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: 4

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

Answer: A

Explanation:

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**Information security governance is PRIMARILY driven by:**

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

Answer: D**Explanation:**

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**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

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's 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

Investments in information security technologies should be based on:

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

Answer: B

Explanation:

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

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.

Answer: B

Explanation:

5

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

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

Answer: B**Explanation:**

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

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.

Answer: B**Explanation:**

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.

Question: 11

Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

- A. Information security manager
- B. Chief operating officer (COO)
- C. Internal auditor
- D. Legal counsel

Answer: B**Explanation:**

The chief operating officer (COO) is highly-placed within an organization and has the most knowledge of business operations and objectives. The chief internal auditor and chief legal counsel are appropriate members of such a steering group. However, sponsoring the creation of the steering committee should be initiated by someone versed in the strategy and direction of the business. Since a security manager is looking to this group for direction, they are not in the best position to oversee formation of this group.

Question: 12

The MOST important component of a privacy policy is:

- A. notifications.
- B. warranties.
- C. liabilities.
- D. geographic coverage.

Answer: A**Explanation:**

Privacy policies must contain notifications and opt-out provisions: they are a high-level management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

Question: 13

The cost of implementing a security control should not exceed the:

- A. annualized loss expectancy.
- B. cost of an incident.
- C. asset value.
- D. implementation opportunity costs.

Answer: C**Explanation:**

The cost of implementing security controls should not exceed the worth of the asset. Annualized loss expectancy represents the losses that are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

Question: 14

When a security standard conflicts with a business objective, the situation should be resolved by:

- A. changing the security standard.
- B. changing the business objective.
- C. performing a risk analysis.
- D. authorizing a risk acceptance.

Answer: C**Explanation:**

Conflicts of this type should be based on a risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. It is highly improbable that a business objective could be changed to accommodate a security standard, while risk acceptance* is a process that derives from the risk analysis.

Question: 15

Minimum standards for securing the technical infrastructure should be defined in a security:

- A. strategy.
- B. guidelines.
- C. model.
- D. architecture.

Answer: D

Explanation:

Minimum standards for securing the technical infrastructure should be defined in a security architecture document. This document defines how components are secured and the security services that should be in place. A strategy is a broad, high-level document. A guideline is advisory in nature, while a security model shows the relationships between components.

Question: 16

Which of the following is MOST appropriate for inclusion in an information security strategy?

- A. Business controls designated as key controls
- B. Security processes, methods, tools and techniques
- C. Firewall rule sets, network defaults and intrusion detection system (IDS) settings
- D. Budget estimates to acquire specific security tools

Answer: B

Explanation:

A set of security objectives, processes, methods, tools and techniques together constitute a security strategy. Although IT and business governance are intertwined, business controls may not be included in a security strategy. Budgets will generally not be included in an information security strategy. Additionally, until information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and intrusion detection system (IDS) settings are technical details subject to periodic change, and are not appropriate content for a strategy document.

Question: 17

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: 18

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: 19

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: 20

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: 21

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: 22

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: 23

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: 24

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: 25

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: 26

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: 27

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: 28

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.

Question: 29

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

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: 30

Relationships among security technologies are BEST defined through which of the following?

- A. Security metrics
- B. Network topology
- C. Security architecture
- D. Process improvement models

Answer: C

Explanation:

Security architecture explains the use and relationships of security mechanisms. Security metrics measure improvement within the security practice but do not explain the use and relationships of security technologies. Process improvement models and network topology diagrams also do not describe the use and relationships of these technologies.

Get Full Version of Exam CISM PDF Q&A

techeXams presents authentic, genuine and valid study material, which promise 100% success in very first attempt. To take optimal results for CISM exam, you need to buy full version of CISM question and answer. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. So come join us and quench your thirst for knowledge.

Get complete CISM exam questions and answers by visiting URL

["http://www.techexams.ws/exams/CISM.do"](http://www.techexams.ws/exams/CISM.do)