**Exam Number/Code :** CISM

**Exam Name:** Certified Information Security Manager

**Version :** Demo

QUESTION 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.

Answer: D

Explanation/Reference:
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 2
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/Reference:
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 economies of scale. However, turnaround can be slower due to the lack of alignment with business units.

QUESTION 3
The MOST important component of a privacy policy is:

A. notifications
B. warranties
C. liabilities

D. geographic coverage

Answer: A

Explanation/Reference:
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 4
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/Reference:
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 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

Answer: A

Explanation/Reference:
The most fundamental evaluation criteria 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
What will have the HIGHEST impact on standard information security governance models?

A. Number of employees
B. Distance between physical locations
C. Complexity of organizational structure
D. Organizational budget

Answer: C

Explanation/Reference:
Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the proper governance.
Organizational budget is not a major impact once good governance models are in place, hence governance will help in effective management of the organization's budget.

QUESTION 7
The PRIMARY goal in developing an information security strategy is to:

A. establish security metrics and performance monitoring.
B. educate business process owners regarding their duties.
C. ensure that legal and regulatory requirements are met.
D. support the business objectives of the organization.

Answer: D

Explanation/Reference:
The business objectives of the organization supersede all other factors. Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

QUESTION 8
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

A. Defining and ratifying the classification structure of information assets
B. Deciding the classification levels applied to the organization's information assets

C. Securing information assets in accordance with their classification
D. Checking if information assets have been classified properly

Answer: A

Explanation/Reference:
Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

QUESTION 9
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.

Answer: B

Explanation/Reference:
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 10
Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

A. Ensure that all IT risks are identified
B. Evaluate the impact of information security risks

C. Demonstrate that IT mitigating controls are in place
D. Suggest new IT controls to mitigate operational risk

Answer: B

Explanation/Reference:
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 11
From an information security manager perspective, what is the immediate benefit of clearly- defined roles and responsibilities?

A. Enhanced policy compliance
B. Improved procedure flows
C. Segregation of duties
D. Better accountability

Answer: D

Explanation/Reference:
Without well-defined roles and responsibilities, there cannot be accountability. Choice A is incorrect because policy compliance requires adequately defined accountability first and therefore is a byproduct. Choice B is incorrect because people can be assigned to execute procedures that are not well designed. Choice C is incorrect because segregation of duties is not automatic, and roles may still include conflicting duties.

QUESTION 12
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

A. Security metrics reports
B. Risk assessment reports
C. Business impact analysis (BIA)
D. Return on security investment report

Answer: B

Explanation/Reference:
Performing a risk assessment will allow the information security manager to prioritize the remedial measures and provide a means to convey a sense of urgency to management. Metrics reports are normally contained within the methodology of the risk assessment to give it credibility and provide an ongoing tool. The business impact analysis (BIA) covers continuity risks only. Return on security investment cannot be determined until a plan is developed based on the BIA.

QUESTION 13
Which of the following is responsible for legal and regulatory liability?

A. Chief security officer (CSO)
B. Chief legal counsel (CLC)
C. Board and senior management
D. Information security steering group

Answer: C

Explanation/Reference:
The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

QUESTION 14
Who in an organization has the responsibility for classifying information?

A. Data custodian
B. Database administrator
C. Information security officer
D. Data owner

Answer: D

Explanation/Reference:
The data owner has full responsibility over data. The data custodian is responsible for securing the information. The database administrator carries out the technical administration. The information security officer oversees the overall classification management of the information.

QUESTION 15
Logging is an example of which type of defense against systems compromise?

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

Answer: B

Explanation/Reference:
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 16
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

Answer: B

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

QUESTION 17
Which of the following factors is a primary driver for information security governance that does not require any further justification?

A. Alignment with industry best practices
B. Business continuity investment
C. Business benefits
D. Regulatory compliance

Answer: D

Explanation/Reference:
Regulatory compliance can be a standalone driver for an information security governance measure. No further analysis nor justification is required since the entity has no choice in the regulatory requirements. Buy-in from business managers must be obtained by the information security manager when an information security governance measure is sought based on its alignment with industry best practices. Business continuity investment needs to be justified by business impact analysis. When an information security governance measure is sought based on qualitative business benefits, further analysis is required to determine whether the benefits outweigh the cost of the information security governance measure in question.

QUESTION 18
A security manager meeting the requirements for the international flow of personal data will need to ensure:

A. a data processing agreement.
B. a data protection registration.
C. the agreement of the data subjects.
D. subject access procedures.

Answer: C

Explanation/Reference:
Whenever personal data are transferred across national boundaries; the awareness and agreement of the data subjects are required. Choices A, B and D are supplementary data protection requirements that are not key for international data transfer.

QUESTION 19
In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

A. prepare a security budget.
B. conduct a risk assessment.
C. develop an information security policy.
D. obtain benchmarking information.

Answer: B

Explanation/Reference:
Risk assessment, evaluation and impact analysis will be the starting point for driving management's attention to information security. All other choices will follow the risk

assessment.

QUESTION 20
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

A. it implies compliance risks.
B. short-term impact cannot be determined.
C. it violates industry security practices.
D. changes in the roles matrix cannot be detected.

Answer: A

Explanation/Reference:
Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.