Exam Code: CISM

Exam Name: Certified Information Security Manager

Vendor: Isaca

Version: DEMO

1: Senior management commitment and support for information security can BEST be obtained through presentations that:
A.use illustrative examples of successful attacks.
B.explains the technical risks to the organization.
C.evaluates the organization against best security practices.
D.ties security risks to key business objectives.
Correct Answers: D

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
Correct Answers: B

3: The MOST important component of a privacy policy is:
A.notifications
B.warranties
C.liabilities
D.geographic coverage
Correct Answers: A

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
Correct Answers: D

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 Answers: A

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
Correct Answers: C

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.
Correct Answers: D

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
Correct Answers: A

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.
Correct Answers: B

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
Correct Answers: B

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
Correct Answers: D

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
Correct Answers: B

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
Correct Answers: C

14: Who in an organization has the responsibility for classifying information?
A.Data custodian
B.Database administrator
C.Information security officer
D.Data owner
Correct Answers: D

15: Logging is an example of which type of defense against systems compromise?
A.Containment
B.Detection
C.Reaction
D.Recovery
Correct Answers: B

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
Correct Answers: B

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
Correct Answers: D

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.
Correct Answers: C

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.
Correct Answers: B

20: emporarily 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.
Correct Answers: A