2021 SPOTO ISACA CISM Practice Questions PDF

1.
Who should be responsible for determining the classification of data within a database used in conjunction with an enterprise application?

A. Database administrator
B. Database architect
C. Data owner
D. Information security manager.

Answer: C

2.
When is the **BEST** time to identify the potential regulatory risk a new service provider presents to the organization?

A. During contract negotiations
B. During integration planning
C. During business case analysis
D. During due diligence

Answer: C

3.
Which of the following defines the **MOST** comprehensive set of security requirements for a newly developed information system?

A. Key risk indicators (KRIs)
B. Audit findings
C. Risk assessment results
D. Baseline controls

Answer: C

4.

Senior management is alarmed by recent media reports of severe security incidents at competing organizations. Which of the following would provide the BEST assurance that the organization's current security measures are performing adequately?

A. Review the intrusion detection system (IDS) logs.
B. Require third-party penetration testing.
C. Require internal penetration testing.
D. Review the intrusion prevention system (IPS) logs.

Answer: B

5.

Which of the following presents the MOST significant challenge when classifying IT assets?

A. Complex asset classification scheme
B. Disagreement between asset owners and custodians
C. Information assets without owners
D. Vulnerabilities in information assets

Answer: C

6.

Senior management has endorsed a comprehensive information security policy. Which of the following should the organization do **NEXT**?

A. implement an authentication and authorization system.
B. Seek policy buy-in from business stakeholders.
C. Identify relevant information security frameworks for adoption.
D. Promote awareness of the policy among employees.

Answer: D

7.

Which of the following should be the GREATEST concern when considering launching a counterattack in response to a network attack?

A. Incident impact escalation

B. Legal ramifications
C. Denial of service attacks on the external source
D. Digital evidence contamination

Answer: B

8.

An organization has remediated a security flaw in a system. Which of the following should be done NEXT?

A. Allocate budget for penetration testing.
B. Update the system's documentation.
C. Assess the residual risk.
D. Share lessons learned with the organization.

Answer: C

9.

An organization has identified an increased threat of external brute force attacks in its environment. Which of the following is the **MOST** effective way to mitigate this risk to the organization's critical systems?

A. Increase the frequency of log monitoring and analysis.
B. Increase the sensitivity of intrusion detection systems.
C. Implement a security information and event management system (SIEM).
D. Implement multi-factor authentication (MFA).

Answer: C

10.

Which of the following should be used to attain sustainable and continuous information security process improvement?

A. Plan, Do, Check, Act Process Model
B. Annual audit
C. Balanced scorecard

D. System development life cycle (SDLC) process

Answer: A

11.

Which of the following **BEST** supports information security management in the event of organizational changes in security personnel?

A. Establishing processes within the security operations team.
B. Developing an awareness program for staff.
C. Ensuring current documentation of security processes.
D. Formalizing a security strategy and program.

Answer: A

12.

An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resources to support clients. What is the BEST approach to obtain the support of business unit management?

A. Discuss the risk and impact of security incidents if not implemented.
B. Elaborate on the positive impact to information security.
C. Present an analysis of the cost and benefit of the changes.
D. Present industry benchmarking results to business units.

Answer: C

13.

An organization has outsourced many application development activities to a third party that uses contract programmers extensively.
Which of the following would provide the **BEST** assurance that the third party's contract programmers comply with the organization's security policies?

A. Include penalties for noncompliance in the contracting agreement.
B. Perform periodic security assessments of the contractors activities.
C. Require annual signed agreements of adherence to security policies.

D. Conduct periodic vulnerability scans of the application.

Answer: D

14.

Which of the following messages would be **MOST** effective in obtaining senior management's commitment to information security management?

A. Security is a business product and not a process.
B. Adopt a recognized framework with metrics.
C. Effective security eliminates risk to the business.
D. Security supports and protects the business.

Answer: D

15.

What should an information security manager do **FIRST** when made aware of a new regulation which may require the redesign of existing information security processes?

A. Develop a future state roadmap.
B. Perform a cost-benefit analysis.
C. Develop a business case.
D. Perform a gap analysis.

Answer: D