- **Vendor:** Isaca
- **Exam Code:** CISM
- **Exam Name:** Certified Information Security Manager
- **New Updated Questions from Braindump2go (Updated in Jnauary/2021)**

QUESTION 1520
An organizations ability to prevent a security incident In a Software as a Service (SaaS) cloud-com pulling environment is MOST dependent on the:

A. ability to implement a web application firewall.
B. ability to monitor and analyze system logs
C. configuration and sensitivity of an intrusion detection system (IDS)
D. granularity with which access rights can be configured

Answer: D

QUESTION 1521
Which of the following would BEST enable effective decision-making?

A. Annualized loss estimates determined from past security events
B. Formalized acceptance of risk analysis by business management
C. A universally applied list of generic threats, impacts, and vulnerabilities
D. A consistent process to analyze new and historical information risk

Answer: D

QUESTION 1522
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 business case analysis
C. During due diligence
D. During integration planning

Answer: B

QUESTION 1523
An awareness program is implemented to mitigate the risk of infections introduced through the use of social media. Which of the following will BEST determine the effectiveness of the awareness program?

A. Employee attendance rate at the awareness program
B. A simulated social engineering attack
C. A post-awareness program survey
D. A quiz based on the awareness program materials

Answer: B

QUESTION 1524
Which of the following security controls should be integrated FIRST into procurement processes to improve the security of the services provided by suppliers?

A. Performing risk assessments to identify security concerns
B. Conducting penetration testing to identify security vulnerabilities
C. Performing regular security audits to determine control deficiencies
D. Creating service contract templates to include security provisions

Answer: D

QUESTION 1525
To meet operational business needs. IT staff bypassed the change process and applied an unauthorized update to a critical business system.
Which of the following is the information security manager's BEST course of action?

A. Assess the security risks introduced by the change.
B. Consult with supervisors of IT staff regarding disciplinary action
C. Update the system configuration item to reflect the change
D. Instruct IT staff to revert the unauthorized update

Answer: A

QUESTION 1526
Which of the following is the information security manager's PRIMARY role in the information assets classification process?

A. Developing an asset classification model
B. Assigning the asset classification level
C. Securing assets in accordance with their classification
D. Assigning asset ownership

Answer: C

QUESTION 1527
When considering whether to adopt bring your own device (BYOD). It is MOST important for the information security manager to ensure that?

A. security controls are applied to each device when joining the network.
B. the applications are tested prior to implementation
C. users have read and signed acceptable use agreements.
D. business leaders have an understanding of security risks

Answer: A

QUESTION 1528
Which of the following is MOST important to include in contracts with key third-party providers?

A. Right-to-audit clauses
B. Financial penalties for breaches
C. Right-to-terminate clauses

D. Provisions to protect sensitive data

Answer: A

QUESTION 1529
Which of the following should be done FIRST when establishing security measures for personal data stored and processed on a human resources....system?

A. Evaluate data encryption technologies.
B. Conduct a vulnerability assessment.
C. Move the system into a separate network.
D. Conduct a privacy impact assessment (PIA).

Answer: D

QUESTION 1530
Risk scenarios simplify the risk assessment process by:

A. reducing the need for subsequent risk evaluation.
B. covering the full range of possible risk.
C. ensuring business risk is mitigated.
D. focusing on important and relevant risk.

Answer: C

QUESTION 1531
Which is MOST important when aligning security priorities with business unit strategies?

A. Risk mitigation plans
B. Stakeholder feedback
C. Gap analysis
D. Business impact analysis (BIA)

Answer: B

QUESTION 1532
What should an information security manager do FIRST after a number of security gaps have been identified that need to be resolved?

A. Develop and implement incident response strategies.
B. Consolidate overlapping controls.
C. Perform a cost-benefit analysis.
D. Prioritize responses based on likelihood and impact.

Answer: D