QUESTION 1412
Which of the following security characteristics is MOST important to the protection of customer data in an online transaction system?

A. Availability
B. Data segregation
C. Audit monitoring
D. Authentication

Answer: D

QUESTION 1413
An organization's information security manager has learned that similar organizations have become increasingly susceptible to spear phishing attacks. What is the BEST way to address this concern?

A. Update data loss prevention (DLP) rules for email.
B. Include tips to identify threats in awareness training.
C. Conduct a business impact analysis (BIA) of the threat.
D. Create a new security policy that staff must read and sign.

Answer: B

QUESTION 1414
What is the PRIMARY benefit to executive management when audit, risk, and security functions are aligned?

A. Reduced number of assurance reports
B. More effective decision making
C. More timely risk reporting
D. More efficient incident handling

Answer: B

QUESTION 1415
A CEO requests access to corporate documents from a mobile device that does not comply with organizational policy. The information security manager should FIRST:

A. evaluate a third-party solution.
B. deploy additional security controls.

C. evaluate the business risk.
D. initiate an exception approval process.

Answer: C

QUESTION 1416
An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:
- A bad actor broke into a business-critical FTP server by brute forcing an administrative password
- The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
- The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
- After three (3) hours, the bad actor deleted the FTP directory causing incoming FTP attempts by legitimate customers to fail
Which of the following poses the GREATEST risk to the organization related to this event?

A. Removal of data
B. Downtime of the service
C. Disclosure of stolen data
D. Potential access to the administration console

Answer: B

QUESTION 1417
An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's FIRST course of action?

A. Shut down the server in an organized manner.
B. Validate that there has been an incident.
C. Inform senior management of the incident.
D. Notify the business process owner.

Answer: B

QUESTION 1418
Which of the following MUST be established before implementing a data loss prevention (DLP) system?

A. Privacy impact assessment
B. A data backup policy
C. Data classification
D. A data recovery policy

Answer: C

QUESTION 1419
An IT department plans to migrate an application to the public cloud. Which of the following is the information security manager's MOST important action in support of this initiative?

A. Calculate security implementation costs.
B. Evaluate service level agreements (SLAs).
C. Provide cloud security requirements.
D. Review cloud provider independent assessment reports.

Answer: B

QUESTION 1420
An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

A. The data owner
B. Internal IT audit
C. The data custodian
D. The information security manager

Answer: D

QUESTION 1421
Who should decide the extent to which an organization will comply with new cybersecurity regulatory requirements?

A. Senior management
B. IT steering committee
C. Legal counsel
D. Information security manager

Answer: A

QUESTION 1422
An information security manager has been alerted to a possible incident involving a breach at one of the organization's vendors. Which of the following should be done FIRST?

A. Discontinue the relationship with the vendor.
B. Perform incident recovery.
C. Perform incident eradication.
D. Engage the incident response team.

Answer: D

QUESTION 1423
Which of the following BEST demonstrates the maturity of an information security monitoring program?

A. Senior management regularly reviews security standards.
B. The information security program was introduced with a thorough business case.
C. Information security key risk indicators (KRIs) are tied to business operations.
D. Risk scenarios are regularly entered into a risk register.

Answer: C

QUESTION 1424
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A. map the business process to supporting IT and other corporate resources.
B. obtain the support of executive management.
C. document the disaster recovery process.
D. identify critical processes and the degree of reliance on support services.

Answer: D

QUESTION 1425
The BEST defense against phishing attempts within an organization is:

A. filtering of e-mail.
B. an intrusion protection system (IPS).
C. strengthening of firewall rules.
D. an intrusion detection system (IDS).

Answer: A

QUESTION 1426
Which of the following should be of GREATEST concern to a newly hired information security manager regarding security compliance?

A. Lack of risk assessments
B. Lack of standard operating procedures
C. Lack of security audits
D. Lack of executive support

Answer: D

QUESTION 1427
Which of the following is the MOST effective way to ensure the process for granting access to new employees is standardized and meets organizational security requirements?

A. Grant authorization to individual systems as required with the approval of information security management.
B. Require managers of new hires be responsible for account setup and access during employee orientation.
C. Embed the authorization and creation of accounts with HR onboarding procedures.
D. Adopt a standard template of access levels for all employees to be enacted upon hiring.

Answer: C

QUESTION 1428
What should an information security team do FIRST when notified by the help desk that an employee's computer has been infected with malware?

A. Take a forensic copy of the hard drive.
B. Restore the files from a secure backup.
C. Isolate the computer from the network.
D. Use anti-malware software to clean the infected computer.

Answer: C

QUESTION 1429
An organization wants to ensure its confidential data is isolated in a multi-tenanted environment at a well- known cloud service provider. Which of the following is the BEST way to ensure the data is adequately protected?

A. Obtain documentation of the encryption management practices.
B. Verify the provider follows a cloud service framework standard.
C. Ensure an audit of the provider is conducted to identify control gaps.
D. Review the provider's information security policies and procedures.

Answer: B

QUESTION 1430
Which of the following BEST enables a more efficient incident reporting process?

A. Training executive management for communication with external entities
B. Educating the incident response team on escalation procedures
C. Educating IT teams on compliance requirements
D. Training end users to identify abnormal events

Answer: D

QUESTION 1431
Which of the following is the MOST important component of a risk profile?

A. Risk management framework
B. Data classification results
C. Penetration test results
D. Risk assessment methodology

Answer: A

QUESTION 1432
When preparing a strategy for protection from SQL injection attacks, it is MOST important for the information security manager to involve:

A. senior management
B. the security operations center.
C. business owners.
D. application developers.

Answer: A

QUESTION 1433
Which of the following is the MOST challenging aspect of securing Internet of Things (IoT) devices?

A. Training staff on IoT architecture
B. Updating policies to include IoT devices
C. Managing the diversity of IoT architecture
D. Evaluating the reputations of IoT vendors

Answer: C

QUESTION 1434
Which of the following is MOST likely to increase end user security awareness in an organization?

A. Simulated phishing attacks
B. Security objectives included in job descriptions
C. Red team penetration testing
D. A dedicated channel for reporting suspicious emails

Answer: B