QUESTION 1347
In an organization where IT is critical to its business strategy and where there is a high level of operational dependence on IT, senior management commitment to security is BEST demonstrated by the:

A. segregation of duties policy
B. size of the IT security function
C. reporting line of the chief information security officer (CISO)
D. existence of an IT steering committee

Answer: D

QUESTION 1348
Which of the following would be an information security manager's PRIMARY challenge when deploying a Bring Your Own Device (BYOD) mobile program in an enterprise?

A. End user acceptance
B. Configuration management
C. Mobile application control
D. Disparate device security

Answer: C

QUESTION 1349
When an operating system is being hardened, it is MOST important for an information security manager to ensure that:

A. system logs are activated
B. default passwords are changed
C. file access is restricted
D. anonymous access is removed

Answer: A

QUESTION 1350
Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?

A. Requiring an external security audit of the IT service provider
B. Defining information security requirements with internal IT

C. Requiring regular reporting from the IT service provider
D. Defining the business recovery plan with the IT service provider

Answer: A

QUESTION 1351
Which of the following would present the GREATEST need to revise information security policies?

A. A merger with a competing company
B. An increase in reported incidents
C. Implementation of a new firewall
D. Changes in standards and procedures

Answer: A

QUESTION 1352
Which of the following MOST effectively prevents internal users from modifying sensitive data?

A. Network segmentation
B. Acceptable use policies
C. Role-based access controls
D. Multi-factor authentication

Answer: C

QUESTION 1353
Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?

A. Number of published application-recovery plans
B. Ratio of recovery-plan documents to total applications
C. Ratio of tested applications to total applications
D. Ratio of successful to unsuccessful tests

Answer: C

QUESTION 1354
Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

A. Holding periodic meetings with business owners
B. Promoting security training
C. Establishing a steering committee
D. Creating communication channels

Answer: C

QUESTION 1355
During an annual security review of an organization's servers, it was found that the customer service team's file server, which contains sensitive customer data, is accessible to all user IDs in the organization. Which of the following should the information security manager do FIRST?

A. Report the situation to the data owner
B. Remove access privileges to the folder containing the data
C. Isolate the server from the network

D. Train the customer service team on properly controlling file permissions

Answer: A

QUESTION 1356
The selection of security controls is PRIMARILY linked to:

A. best practices of similar organizations
B. risk appetite of the organization
C. regulatory requirements
D. business impact assessment

Answer: B

QUESTION 1357
Which of the following is MOST important to include in a contract with a critical service provider to help ensure alignment with the organization's information security program?

A. Right-to-audit clause
B. Escalation paths
C. Key performance indicators (KPIs)
D. Termination language

Answer: C

QUESTION 1358
Which of the following is the BEST reason for delaying the application of a critical security patch?

A. Conflicts with software development lifecycle
B. Technology interdependencies
C. Lack of vulnerability management
D. Resource limitations

Answer: B

QUESTION 1359
Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?

A. Internal audit reports
B. Application security policy
C. Vulnerability assessment results
D. A business case

Answer: D

QUESTION 1360
Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?

A. Improved response time to incidents
B. Improved network protection
C. Enhanced forensic analysis
D. Reduced need for manual analysis

Answer: A

QUESTION 1361
An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST?

A. Application owners
B. Communications department
C. Data owners
D. Security operations team

Answer: D

QUESTION 1362
Which is MOST important when contracting an external party to perform a penetration test?

A. Provide network documentation
B. Obtain approval from IT management
C. Define the project scope
D. Increase the frequency of log reviews

Answer: B

QUESTION 1363
Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files
B. priority of restoration
C. point of synchronization
D. annual loss expectancy (ALE)

Answer: B

QUESTION 1364
Which of the following is an example of a change to the external threat landscape?

A. Infrastructure changes to the organization have been implemented
B. Organizational security standards have been modified
C. A commonly used encryption algorithm has been compromised
D. New legislation has been enacted in a region where the organization does business

Answer: D

QUESTION 1365
Which of the following roles should be PRIMARILY responsible for assigning sensitivity levels to an organization's financial and payroll databases?

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

Answer: A

QUESTION 1366

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

A. the importance of the functional to be tested and the cost of testing
B. the experience level of personnel and the function location
C. prior testing results and the degree of detail of the business continuity plan
D. manual processing capabilities and the test location

Answer: A

QUESTION 1367
A policy has been established requiring users to install mobile device management (MDM) software on their personal devices. Which of the following would BEST mitigate the risk created by noncompliance with this policy?

A. Issuing warnings and documenting noncompliance
B. Requiring users to sign off on terms and conditions
C. Issuing company-configured mobile devices
D. Disabling remote access from the mobile device

Answer: D