QUESTION 1326
Which of the following is MOST critical to review when preparing to outsource a data repository to a cloud- based solution?

A. Disaster recovery plan
B. Identity and access management
C. Vendor's information security policy
D. A risk assessment

Answer: C

QUESTION 1327
Which of the following is MOST useful to include in a report to senior management on a regular basis to demonstrate the effectiveness of the information security program?

A. Key risk indicators (KRIs)
B. Capability maturity models
C. Critical success factors (CSFs)
D. Key performance indicators (KPIs)

Answer: A

QUESTION 1328
Which of the following is the MOST important factor when determining the frequency of information security reassessment?

A. Risk priority
B. Risk metrics
C. Audit findings
D. Mitigating controls

Answer: B

QUESTION 1329
Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?

A. Risk assessment
B. Business impact analysis (BIA)

C. Penetration testing
D. Gap analysis

Answer: D

QUESTION 1330
Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?

A. Integrate industry best practices
B. Obtain senior management sign-off
C. Conduct an organization-wide security audit
D. Leverage security steering committee contribution

Answer: D

QUESTION 1331
In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?

A. Conduct a business impact analysis (BIA) and provide the report to management.
B. Update the corporate mobile usage policy to prohibit texting.
C. Stop providing mobile devices until the organization is able to implement controls.
D. Include the topic of prohibited texting in security awareness training.

Answer: D

QUESTION 1332
Which of the following is the BEST approach for determining the maturity level of an information security program?

A. Evaluate key performance indicators (KPIs)
B. Engage a third-party review
C. Review internal audit results
D. Perform a self-assessment

Answer: A

QUESTION 1333
A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

A. using a secret key in conjunction with the hash algorithm
B. requiring the recipient to use a different hash algorithm
C. using the sender's public key to encrypt the message
D. generating hash output that is the same size as the original message

Answer: A

QUESTION 1334
An organization's marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risks assessment. Which of the following should be the MOST important consideration?

A. The information to be exchanged

B. Methods for transferring the information
C. Reputations of the external marketing companies
D. The security of the third-party cloud provider

Answer: B

QUESTION 1335
What should the information security manager do FIRST when end users express that new security controls are too restrictive?

A. Conduct a business impact analysis (BIA)
B. Obtain process owner buy-in to remove the controls
C. Perform a risk assessment on modifying the control environment
D. Perform a cost-benefit analysis on modifying the control environment

Answer: C

QUESTION 1336
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

A. Analyze vulnerabilities
B. Determine recovery priorities
C. Confirm control effectiveness
D. Define the recovery point objective (RPO)

Answer: D

QUESTION 1337
An organization implemented a mandatory information security awareness training program a year ago.
What is the BEST way to determine its effectiveness?

A. Analyze findings from previous audit reports
B. Analyze results from training completion reports
C. Analyze results of a social engineering test
D. Analyze responses from an employee survey of training satisfaction

Answer: C

QUESTION 1338
Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?

A. Requiring periodic self-assessments by the provider
B. Evaluating the provider's security incident response plan
C. Continuous monitoring of an information security risk profile
D. Ensuring the provider's roles and responsibilities are established

Answer: C

QUESTION 1339
An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?

A. Perform regular audits on the implementation of critical patches.

B. Evaluate patch management training.
C. Assess the patch management process.
D. Monitor and notify IT staff of critical patches.

Answer: C

QUESTION 1340
A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the BEST way to obtain assurance that the provider can adequately protect the organization's information?

A. Invoke the right to audit per the contract
B. Review the provider's information security policy
C. Check references supplied by the provider's other customers
D. Review the provider's self-assessment

Answer: A

QUESTION 1341
Which of the following is MOST important when selecting an information security metric?

A. Aligning the metric to the IT strategy
B. Defining the metric in quantitative terms
C. Ensuring the metric is repeatable
D. Defining the metric in qualitative terms

Answer: B

QUESTION 1342
Which of the following BEST supports the risk assessment process to determine criticality of an asset?

A. Business impact analysis (BIA)
B. Residual risk analysis
C. Vulnerability assessment
D. Threat assessment

Answer: A

QUESTION 1343
When recommending a preventive control against cross-site scripting in web applications, an information security manager is MOST likely to suggest:

A. using https in place of http
B. coding standards and code review
C. consolidating multiple sites into a single portal
D. hardening of the web server's operating system

Answer: B

QUESTION 1344
The PRIMARY benefit of integrating information security activities into change management processes is to:

A. ensure required controls are included in changes
B. protect the organization from unauthorized changes
C. provide greater accountability for security-related changes in the business

D. protect the business from collusion and compliance threats

Answer: A

QUESTION 1345
Which of the following should be an information security manager's MOST important consideration when conducting a physical security review of a potential outsourced data center?

A. Distance of the data center from the corporate office
B. Availability of network circuit connections
C. Environment factors of the surrounding location
D. Proximity to law enforcement

Answer: C

QUESTION 1346
Which of the following tools BEST demonstrates the effectiveness of the information security program?

A. Key risk indicators (KRIs)
B. Management satisfaction surveys
C. Risk heat map
D. A security balanced scorecard

Answer: D