QUESTION 1389
Which of the following is the MOST beneficial outcome of testing an incident response plan?

A. Test plan results are documented
B. The plan is enhanced to reflect the findings of the test
C. Incident response time is improved
D. The response includes escalation to senior management

Answer: C

QUESTION 1390
Following a malicious security incident, an organization has decided to prosecute those responsible. Which of the following will BEST facilitate the forensic investigation?

A. Performing a backup of affected systems
B. Identifying the affected environment
C. Maintaining chain of custody
D. Determining the degree of loss

Answer: C

QUESTION 1391
Which of the following is the MOST important factor to consider when establishing a severity hierarchy for information security incidents?

A. Regulatory compliance
B. Business impact
C. Management support
D. Residual risk

Answer: B

QUESTION 1392
Which of the following is the MOST important reason to document information security incidents that are reported across the organization?

A. Identify unmitigated risk
B. Prevent incident recurrence

C. Evaluate the security posture of the organization
D. Support business investments in security

Answer: B

QUESTION 1393
Which of the following is the MOST important part of an incident response plan?

A. Recovery time objective (RTO)
B. Business impact analysis (BIA)
C. Recovery point objective (RPO)
D. Mean time to report (MTTR)

Answer: A

QUESTION 1394
When designing an incident response plan to be agreed upon with a cloud computing vendor, including which of the following will BEST help to ensure the effectiveness of the plan?

A. A training program for the vendor staff
B. An audit and compliance program
C. Responsibility and accountability assignments
D. Requirements for onsite recovery testing

Answer: C

QUESTION 1395
Following a highly sensitive data breach at a large company, all servers and workstations were patched. The information security manager's NEXT step should be to:

A. inform senior management of changes in risk metrics.
B. perform an assessment to measure the current state.
C. deliver security awareness training.
D. ensure baseline back-ups are performed.

Answer: B

QUESTION 1396
The MOST important reason for an information security manager to be involved in the change management process is to ensure that:

A. security controls are updated regularly.
B. potential vulnerabilities are identified.
C. risks have been evaluated.
D. security controls drive technology changes.

Answer: D

QUESTION 1397
The PRIMARY purpose of implementing information security governance metrics is to:

A. measure alignment with best practices.
B. assess operational and program metrics.
C. refine control operations,

D. guide security towards the desired state.

Answer: D

QUESTION 1398
Which of the following is the information security manager's PRIMARY role in the information assets classification process?

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

Answer: D

QUESTION 1399
Cold sites for disaster recovery events are MOST helpful in situations in which a company:

A. has a limited budget for coverage.
B. uses highly specialized equipment that must be custom manufactured.
C. is located in close proximity to the cold site.
D. does not require any telecommunications connectivity

Answer: A

QUESTION 1400
Which of the following processes would BEST aid an information security manager in resolving systemic security issues?

A. Root cause analysis
B. Business impact analysis (BIA)
C. Reinforced security controls
D. Security reviews

Answer: A

QUESTION 1401
Which of the following is MOST important when carrying out a forensic examination of a laptop to determine an employee's involvement in a fraud?

A. The employee's network access should be suspended.
B. The laptop should not be removed from the company premises.
C. An HR representative should be present during the laptop examination.
D. The investigation should be conducted on an image of the original disk drive.

Answer: D

QUESTION 1402
What should be the PRIMARY basis for establishing a recovery time objective (RTO) for a critical business application?

A. Business impact analysis (BIA) results
B. Related business benchmarks
C. Risk assessment results
D. Legal and regulatory requirements

Answer: A

QUESTION 1403
Which of the following BEST supports the alignment of information security with business functions?

A. Creation of a security steering committee
B. IT management support of security assessments
C. Business management participation in security penetration tests
D. A focus on technology security risk within business processes

Answer: A

QUESTION 1404
Which of the following should be done FIRST when handling multiple confirmed incidents raised at the same time?

A. Activate the business continuity plan (BCP).
B. Update the business impact assessment.
C. Inform senior management.
D. Categorize incidents by the value of the affected asset.

Answer: D

QUESTION 1405
An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?

A. Invoke the organization's incident response plan.
B. Set up communication channels for the target audience.
C. Determine the needs and requirements of each audience.
D. Create a comprehensive singular communication.

Answer: C

QUESTION 1406
An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's FIRST course of action?

A. Report the noncompliance to the board of directors.
B. Inform respective risk owners of the impact of exceptions
C. Design mitigating controls for the exceptions.
D. Prioritize the risk and implement treatment options.

Answer: D

QUESTION 1407
Which of the following is the MOST effective method for categorizing system and data criticality during the risk assessment process?

A. Interview senior management.
B. Interview data custodians.
C. Interview members of the board.
D. Interview the asset owners.

Answer: D

QUESTION 1408
Which of the following features of a library control software package would protect against unauthorized updating of source code?

A. Required approvals at each life cycle step
B. Date and time stamping of source and object code
C. Access controls for source libraries
D. Release-to-release comparison of source code

Answer: C

QUESTION 1409
An organization plans to leverage popular social network platforms to promote its products and services. Which of the following is the BEST course of action for the information security manager to support this initiative?

A. Develop security controls for the use of social networks
B. Assess the security risk associated with the use of social networks
C. Establish processes to publish content on social networks
D. Conduct vulnerability assessments on social network platforms

Answer: C

QUESTION 1410
When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure that the:

A. server is backed up to the network.
B. server is unplugged from power.
C. integrity of evidence is preserved.
D. forensic investigation software is loaded on the server.

Answer: C

QUESTION 1411
When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?

A. Recommendations from senior management
B. The business continuity plan (BCP)
C. Business impact analysis (BIA) results
D. Vulnerability assessment results

Answer: C