QUESTION 1368
The PRIMARY purpose of a periodic threat and risk assessment report to senior management is to communicate the:

A. status of the security posture
B. probability of future incidents
C. cost-benefit of security controls
D. risk acceptance criteria

Answer: A

QUESTION 1369
An organization's HR department would like to outsource its employee system to a cloud-hosted solution due to features and cost savings offered. Management has identified this solution as a business need and wants to move forward. What should be the PRIMARY role of information security in this effort?

A. Explain security issues associated with the solution to management
B. Determine how to securely implement the solution
C. Ensure the service provider has the appropriate certifications
D. Ensure a security audit is performed of the service provider

Answer: B

QUESTION 1370
Which of the following is MOST effective against system intrusions?

A. Two-factor authentication
B. Continuous monitoring
C. Layered protection
D. Penetration testing

Answer: C

QUESTION 1371
What should be the information security manager's MOST important consideration when planning a disaster recovery test?

A. Documented escalation processes
B. Organization-wide involvement

C. Impact to production systems
D. Stakeholder notification procedures

Answer: C

QUESTION 1372
The PRIMARY purpose of asset valuation for the management of information security is to:

A. prioritize risk management activities
B. eliminate the least significant assets
C. provide a basis for asset classification
D. determine the value of each asset

Answer: D

QUESTION 1373
The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:

A. security program priorities to achieve an accepted risk level
B. level of compliance with internal policy
C. assessed level of security risk at a particular point in time
D. current and target security state for the business

Answer: D

QUESTION 1374
Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?

A. Identifying risk mitigation options
B. Identifying critical business processes
C. Identifying key business risks
D. Identifying the threat environment

Answer: C

QUESTION 1375
An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the BEST way to address this situation?

A. Report the risk and status of the information security program to the board
B. Revise the information security strategy to meet executive management's expectations
C. Escalate noncompliance concerns to the internal audit manager
D. Demonstrate alignment of the information security function with business needs

Answer: D

QUESTION 1376
The MOST important reason that security risk assessments should be conducted frequently throughout an organization is because:

A. control effectiveness may weaken
B. compliance with legal and regulatory standards should be reassessed
C. controls should be regularly tested

D. threats to the organization may change

Answer: D

QUESTION 1377
A recent audit has identified that security controls by the organization's policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?

A. Discuss the issue with the data owners to determine the reason for the exception
B. Discuss the issue with data custodians to determine the reason for the exception
C. Report the issue to senior management and request funding to fix the issue
D. Deny access to the application until the issue is resolved

Answer: A

QUESTION 1378
Which of the following is the PRIMARY role of a data custodian?

A. Validating information
B. Processing information
C. Classifying information
D. Securing information

Answer: D

QUESTION 1379
The MAIN consideration when designing an incident escalation plan should be ensuring that:

A. appropriate stakeholders are involved
B. information assets are classified
C. requirements cover forensic analysis
D. high-impact risks have been identified

Answer: A

QUESTION 1380
Which of the following should be the PRIMARY objective of the information security incident response process?

A. Conducting incident triage
B. Classifying incidents
C. Communicating with internal and external parties
D. Minimizing negative impact to critical operations

Answer: D

QUESTION 1381
Which of the following is the PRIMARY purpose of red team testing?

A. To determine the organization's preparedness for an attack
B. To assess the vulnerability of employees to social engineering
C. To establish a baseline incident response program
D. To confirm the risk profile of the organization

Answer: A

QUESTION 1382
Which of the following external entities would provide the BEST guidance to an organization facing advanced attacks?

A. Recognized threat intelligence communities
B. Open-source reconnaissance
C. Disaster recovery consultants widely endorsed in industry forums
D. Incident response experts from highly regarded peer organizations

Answer: D

QUESTION 1383
An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the BEST course of action to address this issue?

A. Activate the organization's incident response plan
B. Include security requirements in outsourcing contracts
C. Terminate the agreement with the third-party contractor
D. Limit access to the third-party contractor

Answer: A

QUESTION 1384
Which of the following is the MOST important reason for logging firewall activity?

A. Incident investigation
B. Auditing purposes
C. Intrusion detection
D. Firewall tuning

Answer: A

QUESTION 1385
Which of the following is the BEST way to improve the timely reporting of information security incidents?

A. Perform periodic simulations with the incident response team
B. Integrate an intrusion detection system (IDS) in the DMZ
C. Incorporate security procedures in help desk processes
D. Regularly reassess and update the incident response plan

Answer: B

QUESTION 1386
What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?

A. Establish and measure key performance indicators (KPIs)
B. Communicate incident response procedures to staff
C. Test incident response procedures regularly
D. Obtain senior management commitment

Answer: A

QUESTION 1387

When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?

A. Post-incident analysis results
B. The risk management process
C. The security awareness programs
D. Firewall logs

Answer: B

QUESTION 1388
An information security manager is developing evidence preservation procedures for an incident response plan. Which of the following would be the BEST source of guidance for requirements associated with the procedures?

A. IT management
B. Legal counsel
C. Executive management
D. Data owners

Answer: D