QUESTION 1704
A company is considering a new automated system that requires implementation of wireless devices for data capture. Even though wireless is not an approved technology, senior management has accepted the risk and approved a Proof-of-Concept (POC) to evaluate the technology and proposed solution. Which of the following is the information security manager's BEST course of action?

A. Develop corporate wireless standards.
B. Implement a wireless intrusion detection system (IDS).
C. Provide personnel with wireless security training.
D. Sandbox the proposed solution.

Answer: A

QUESTION 1705
Which of the following is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business?

A. Information security governance
B. Risk assessment program
C. Information security metrics
D. Information security awareness training

Answer: A

QUESTION 1706
For which of the following is it MOST important that system administrators be restricted to read-only access?

A. User access log files
B. Administrator user profiles
C. System logging options
D. Administrator log files

Answer: A

QUESTION 1707
Which of the following would BEST help an information security manager justify the implementation ofa security information and event management (SIEM) system?

A. Results of a risk assessment

B. Results of a cost-benefit analysis
C. Security benchmarks
D. Results of a business impact analysis (BIA)

Answer: B

QUESTION 1708
Which of the following would BEST help to ensure the alignment between information security and business functions?

A. Establishing a security awareness program
B. Establishing an information security governance committee
C. Providing funding for information security efforts
D. Developing information security policies

Answer: B

QUESTION 1709
Effective information security policies should be PRIMARILY developed based on:

A. industry best practices.
B. the ease of enforcement.
C. the cost of implementation,
D. the organization's risk profile.

Answer: B

QUESTION 1710
Which of the following BEST reflects the maturity of an information security program?

A. The number of security issues reported
B. The number of security incidents detected
C. The number of policies traceable to usable metrics
D. The number of findings corrected annually

Answer: C

QUESTION 1711
Labeling information according to its security classification:

A. reduces the need to identify baseline controls for each classification.
B. reduces the number and type of countermeasures required.
C. affects the consequences if information is handled insecurely.
D. enhances the likelihood of people handling information securely.

Answer: D

QUESTION 1712
Which of the following would be MOST helpful to identify security incidents in a timely manner?

A. Develop 4 user awareness program.
B. Require security staff to attend training.
C. implement a ticketing system for the help desk.
D. Perform regular penetration testing.

Answer: A

QUESTION 1713
Which of the following is MOST important to implement when using a service account for infrastructure administration?

A. Audit trail
B. Password control
C. Account lockout
D. Hash totals

Answer: B

QUESTION 1714
An organization has implemented a bring your own device (BYOD)} program. hich of the following is the GREATEST risk to the organization?

A. Lack of nonrepudiation
B. Device theft
C. Device incompatibility
D. Data leakage

Answer: B

QUESTION 1715
During a security assessment, an information security manager finds a number of security patches were not installed on a server hosting a critical business application. The application owner did not approve the patch installation to avoid interrupting the application. Which of the following should be the information security manager's FIRST course of action?

A. Determine mitigation options with IT management
B. Communicate the potential impact to the application owner.
C. Report the risk to the information security steering committee.
D. Escalate the risk to senior management.

Answer: B

QUESTION 1716
Which of the following is the MOST important consideration in a bring your own device (BYOD) program to protect company data in the event of a loss?

A. The ability to centrally manage devices
B. The ability to remotely locate devices
C. The ability to classify types of devices
D. The ability to restrict unapproved applications

Answer: A

QUESTION 1717
Which of the following should be part of the final phase of an incident response plan?

A. Recovering the impacted system
B. Performing a system rollback
C. Updating the risk register
D. Reviewing lessons learned

Answer: D

QUESTION 1718
Which of the following is the BEST method for determining whether new risks exist in legacy systems?

A. Regularly scheduled security audits
B. Regularly scheduled risk assessments
C. Frequent updates to the risk register
D. Automated vulnerability scans

Answer: D

QUESTION 1719
Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Require users to acknowledge the acceptable use policy.
B. Base mandatory review and exception approvals on inherent risk.
C. Require the steering committee to review exception requests
D. Base mandatory review and exception approvals on residual risk.

Answer: D

QUESTION 1720
Which of the following is the GREATEST benefit of an information security architecture?

A. Closer integration with the incident response team function
B. Alignment with industry best practices
C. Ease of integration between different security components
D. Fewer false positives in the security incident and event management (SIEM)

Answer: C

QUESTION 1721
What should an information security manager do FIRST upon learning of a significant regulatory change that impacts how the organization should safeguard critical data?

A. Perform a gap analysis.
B. Report the regulatory change to senior management
C. Implement needed control changes.
D. Assess impact to industry peers.

Answer: A

QUESTION 1722
Which of the following should be done FIRST when implementing an information security strategy?

A. Map business goals to information security strategy objectives.
B. Benchmark the strategy with industry peers.
C. Identify owners of information assets
D. Determine the desired state of information security.

Answer: D

QUESTION 1723
Which of the following should an information security manager consider when reviewing an existing security investment plan?

A. The plan is based on a review of threats. and vulnerabilities in existing IT systems.
B. The plan focuses on meeting industry best practices and industry standards.
C. The plan identifies all potential threats and their impact on business processes
D. The plan has summarized IT costs for implementation.

Answer: A

QUESTION 1724
Which of the following methods is the BEST way to demonstrate that an information security program provides appropriate coverage?

A. Maturity assessment
B. Security risk analysis
C. Vulnerability scan report
D. Gap assessment

Answer: D

QUESTION 1725
Which of the following is the MOST efficient tool for identifying advanced persistent threats (APTs)?

A. Security incident and event management (SIEM) tool
B. Web application firewall
C. Intrusion detection system (IDS)
D. Internet gateway filter

Answer: A

QUESTION 1726
Which of the following is the MOST important consideration when designing a disaster recovery test?

A. The test fully recovers the storage infrastructure
B. The test assesses the adequacy of network redundancy.
C. The test includes the recovery time objectives (RTOs).
D. The test addresses critical business functions.

Answer: D

QUESTION 1727
An organization must meet rigorous breach reporting standards in order to comply with regulatory requirements. Which of the following is the BEST way to minimize the organization's financial exposure if a service provider experiences a breach?

A. Include the reporting requirements in the provider contract.
B. Require the provider to comply with organization's information security policy.
C. Review the reporting requirements and processes contained in the provider's policies.
D. Verify the provider has automated reporting processes in place.

Answer: A

QUESTION 1728
A senior executive asks the information security manager to bypass the organization's Internet traffic filters due to a business need.
Which of the following should be the information security manager's NEXT course of action?

A. Deny the request as noncompliant with policy
B. Accept the request immediately based on the business criticality.
C. Notify the IT network manager and make an approval decision jointly.
D. Document the risk and mark for future review.

Answer: D

QUESTION 1729
An intrusion prevention system (IPS) has reported a significant increase in the number of hacking attempts over the past month,
though no systems have actually been compromised. Which of the following should the information security manager do FIRST?

A. Report the increase in hacking attempts to senior management.
B. Validate the events identified by the IPS.
C. Add more resources to monitor IPS alerts.
D. Assess the risk associated with the hacking attempts.

Answer: B

QUESTION 1730
Which of the following is the MOST important reason for an organization to communicate to affected parties that a security has occurred?

A. To improve awareness of information security
B. To disclose the root cause of the incident
C. To increase goodwill towards the organization
D. To comply with regulations regarding notification

Answer: D

QUESTION 1731
When developing metrics related to an organization's information security program, what information will provide the MOST value to enable strategic decision-making?

A. How many security incidents are reported each month
B. How well information security risk is being predicted
C. How long it takes security incidents to be closed
D. How frequently the information security risk register is updated

Answer: B

QUESTION 1732
An organization Is storing accounting data in an external cloud environment. Which of the following is the MOST important riskrelated consideration?

A. Availability of audit logs
B. Access to physical servers hosting the data
C. Access authorization to the data

D. Data backup capabilities

Answer: C

QUESTION 1733
Which of the following is the MOST important factor of a successful information security program?

A. The program is based on a well-developed strategy.
B. The program is focused on risk management.
C. The program follows industry best practices
D. The program is cost-efficient and within budget.

Answer: A

QUESTION 1734
An information security manager is reviewing a contract with a third-party service provider. Which of the following issues should be of MOST concerm?

A. The provider lacks compliance certification.
B. Penalties for breach of contract are not defined.
C. The provider states the client is responsible for data classification.
D. There is no provision for a right to audit.

Answer: B

QUESTION 1735
Which of the following is the PRIMARY objective of an incident response plan?

A. To communicate escalation procedures
B. To minimize business disruption
C. To establish appropriate service level agreements (SLAs)
D. To define roles and responsibilities

Answer: B

QUESTION 1736
An organization has acquired a new system with strict maintenance instructions and schedules.
Where should this information be documented?

A. Procedures
B. Guidelines
C. Policies
D. Standards

Answer: A

QUESTION 1737
What should be the PRIMARY basis for developing an organization's information security program?

A. Customer service strategy
B. Organizational strategy
C. Information security strategy
D. Regulatory compliance strategy

Answer: C

QUESTION 1738
An organization recently experienced a ransomware attack. What is the BEST course of action to reduce the likelihood of successful future attacks?

A. Recalibrate the intrusion prevention system (IPS).
B. Provide employees with security awareness training.
C. Update antivirus definition files.
D. Block Internet access to websites that are not work-related.

Answer: B

QUESTION 1739
Which of the following is the BEST indication that the information security strategy is delivering business value?

A. Stakeholders regularly seek feedback from the information security team
B. Key risk indicators (KRIs) are regularly reviewed.
C. The information security team analyzes results from end user surveys.
D. There has been a significant reduction in the number of reported incidents.

Answer: D

QUESTION 1740
Which of the following BEST prepares an organization for disaster recovery?

A. Failover testing
B. Help desk training
C. Penetration testing
D. An incident response policy

Answer: D

QUESTION 1741
Which of the following is the PRIMARY reason for conducting post-incident reviews?

A. To determine the level of required remediation
B. To establish the cost of remediation
C. To ensure regulatory compliance
D. To review lessons learned

Answer: D

QUESTION 1742
An organization has selected an internationally recognized information security framework. Which of the following should be the PRIMARY basis for prioritizing the creation of related policies?

A. Budgetary requirements to support implementation
B. Steering committee recommendations
C. Regulatory requirements
D. Correlation to business strategy

Answer: D

QUESTION 1743
Who should have PRIMARY responsibility for authorizing access to data residing in an enterprise resource application?

A. Application administrator
B. Data custodian
C. Identity and access management team
D. Process owner

Answer: D

QUESTION 1744
Which of the following is MOST important to establish when developing prioritization processes for events during an incident?

A. Recovery point objective (RPO)
B. Recovery time objective (RTO)
C. Security management approval
D. Criteria for alerting senior management

Answer: B

QUESTION 1745
Which of the following is MOST useful when prioritizing information security initiatives?

A. Cost of noncompliance
B. Risk assessment results
C. Input from senior management
D. Penetration testing results

Answer: B

QUESTION 1746
The MOST significant outcome obtained from conducting a business impact analysis (BIA) is improved:

A. IT capacity planning.
B. disaster recovery planning.
C. data center design.
D. incident response planning.

Answer: D

QUESTION 1747
Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?

A. Update disciplinary processes to address privacy violations
B. Create an inventory of systems where personal data is stored
C. Evaluate privacy technologies required for data protection
D. Encrypt all personal data stored on systems and networks

Answer: B

QUESTION 1748
Which of the following BEST enables senior management to monitor the organization's risk exposure?

A. Monthly reporting on changes to the risk profile .
B. Monthly reporting on information security incidents.
C. Monthly reporting on new threats and vulnerabilities
D. Monthly reporting on the IT risk register

Answer: A

QUESTION 1749
Which of the following will ensure confidentiality of content when accessing an email system over the Internet?

A. Digital encryption
B. Data masking
C. Digital signatures
D. Multifactor authentication (MFA)

Answer: A

QUESTION 1750
Which of the following is the BEST methodology to manage access rights?

A. Mandatory access control
B. Zero trust model
C. Two-factor authentication
D. Discretionary access control

Answer: B

QUESTION 1751
An information security team has identified traffic from a device to a known malicious IP. Which of the following should be the team's FIRST course of action to address this issue?

A. Turn off the device.
B. Run anti-malware software on the device.
C. Re-image the device.
D. Disconnect the device from the network.

Answer: D

QUESTION 1752
Which of the following is an information security manager's BEST course of Action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?

A. Assess the risk to the organization.
B. Notify staff members of the threat.
C. Increase the frequency of system backups.
D. Review the mitigating security controls.

Answer: B

QUESTION 1753
When evaluating cloud storage solutions, the FIRST consideration should be

A. alignment with the organization's classification policy.

B. how the organization's sensitive data will be transferred.
C. Who controls the encryption keys.
D. The level of protection of data stored in the cloud

Answer: D

QUESTION 1754
A corporate laptop containing confidential data is compromised The incident has been contained, and the laptop is in the possession of the incident response team The NEXT step should be to

A. Create a duplicate image.
B. Initiate system recovery.
C. Wipe the system.
D. Dispose of the laptop hard drive.

Answer: A

QUESTION 1755
Which of the following is the BEST evidence of the maturity of an organization's information security program?

A. IT security staff implements strict technical security controls.
B. The number of reported incidents has increased.
C. Management has approved the information security policy.
D. The number of reported incidents has decreased.

Answer: C

QUESTION 1756
An organization has acquired a company in a foreign country to gain an advantage in a new market Which of the following is the FIRST step the information security manager should take?

A. Apply the existing information security program to the acquired company.
B. Evaluate the information security laws that apply to the acquired company.
C. Merge the two existing information security programs.
D. Determine which country's information security regulations will be used.

Answer: B

QUESTION 1757
An organization's head of information security has been tasked with creating an information security strategy What is the MOST important reason to include business representation?

A. To support business goals.
B. To establish an enterprise security architecture
C. To identify business risk owners
D. To facilitate a business impact analysis (BIA)

Answer: A

QUESTION 1758
Which is the BEST method to evaluate the effectiveness of an alternate processing site when continuous uptime is required?

A. Full interruption test

B. Tabletop test
C. Simulation test
D. Parallel test

Answer: D

QUESTION 1759
An organization has launched a new function on its company website to enable customers to purchase products online using credit cards Which of the following will BEST help to ensure credit card information is secure? The credit card information is

A. processed and stored in a separate data center.
B. Stored in the same country in which the company operates.
C. Masked when displayed online.
D. Encrypted when in transit and at rest.

Answer: D

QUESTION 1760
To help users apply appropriate controls related to data privacy regulation, what is MOST important to communicate to the users?

A. Data classification policy
B. Data storage procedures
C. Features of data protection products
D. Results of penetration testing

Answer: A

QUESTION 1761
Which of the following is MOST important to the success of an incident response team?

A. Skilled personnel with technical expertise
B. Annual end user awareness training
C. The completion of tabletop exercises
D. Management approval of test plans

Answer: D

QUESTION 1762
Which of the following would BEST enable an information security manager to identify the risk associated with cloud-based solutions?

A. Benchmarking with peer organizations using cloud solutions
B. Assessing the solutions against the organization's security policies
C. Reviewing vendor adherence to service level agreements (SLAs)
D. Reviewing third-party audits of cloud service providers

Answer: B

QUESTION 1763
Which of the following is MOST useful to help hold vendors accountable for security practices?

A. An overview of the organization's security processes

B. Requirements for independent reviews
C. A copy of the information security policy
D. Security-related contract clauses

Answer: D

QUESTION 1764
Which of the following BEST demonstrates return on investment (ROI) for an information security initiative?

A. Information security program roadmap
B. Business impact analysis (BIA)
C. Business case
D. Risk heat map

Answer: B

QUESTION 1765
Which of the following provides an information security manager with the MOST accurate indication of the organization's ability to respond to a cyber attack?

A. Walk-through of the incident response plan
B. Red team exercise
C. Simulated phishing exercise
D. Black box penetration test

Answer: B

QUESTION 1766
The BEST way to identify the risk associated with a social engineering attack is to An organization has acquired a company that manufactures Internet of Things (loT) devices What should the information security manager do NEXT?

A. Update the information security strategy.
B. Review the acquired company's data sharing agreements.
C. Review the acquired company's audit reports.
D. Conduct a vulnerability assessment.

Answer: B

QUESTION 1767
The BEST way to identify the risk associated with a social engineering attack is to

A. Review single sign-on authentication logs.
B. Perform a business risk assessment of the email filtering system.
C. Monitor the intrusion detection system (IDS)
D. Test user knowledge of information security practices.

Answer: D

QUESTION 1768
For workstations used to facilitate a forensic investigation it is MOST important to ensure

A. The workstations are backup up and hardened on a regular basis
B. the workstations are only accessed by members of the forensics team
C. a documented chain of custody log is kept for the workstations.

D. only forensics-related software is installed on the workstations

Answer: C

QUESTION 1769
Which of the following is the BEST way for senior leadership to demonstrate commitment for an effective Information security strategy?

A. Communicating organization risk appetite and tolerance
B. Appointing the top information security role to report to the CEO
C. Allocating adequate resources for information security
D. Approving a comprehensive risk management program

Answer: C

QUESTION 1770
Which of the following is the BEST indication that information security is integrated into corporate governance?

A. New vulnerably are reported directly to the security manager.
B. Significant incidents are escalated to executive management.
C. Administrative staff is trained on current information security topics.
D. Security policy documents are reviewed periodically.

Answer: B

QUESTION 1771
Which of the following would provide the MOST effective security outcome in an organization s contract management process?

A. Performing vendor security benchmark analyses at the request-for proposal (FRP) stage
B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage.
C. Extending security assessment to cover asset disposal on contract termination
D. Extending security assessment to include random penetration testing

Answer: B

QUESTION 1772
Which of the following should be the PRIMARY objective when establishing a new information security program?

A. Executing the security strategy
B. Optimizing resources
C. Facilitating operational security
D. Achieving regulatory compliance

Answer: A

QUESTION 1773
To minimize the business impact from information security incidents it is MOST important to

A. Attain timely identification of incidents.
B. Streamline the post-incident review process.
C. Keep all incident-related data confidential.
D. reduce staff costs for incident recovery

Answer: A

QUESTION 1774
Which of the following is the BEST way to ensure that responses to incidents in high-risk areas of the business are earned out m an organized manner?

A. Management approval of the incident response plan
B. Role differentiation in the incident response plan
C. Appropriate communication of the incident response plan
D. Periodic testing of the incident response plan

Answer: D

QUESTION 1775
Which of the following BEST enables an information security manager to assess the effectiveness of the information security program?

A. Penetration testing results
B. Risk register
C. Maturity level
D. Information security architecture

Answer: C

QUESTION 1776
Which of the following is MOST important for guiding the development and management of a comprehensive information security program?

A. Establishing and maintaining an information security governance framework
B. Adopting information security program management best practices
C. Implementing policies and procedures to address the information security strategy
D. Aligning the organization's business objectives with IT objectives

Answer: A

QUESTION 1777
A data loss prevention (DLP) tool has flagged personally identifiable information (Pll) during transmission. Which of the following should the information security manager do FIRST?

A. Escalate the issue to senior management.
B. Notify authorities and the cyber insurance company
C. Validate the scope and Impact with the business process owner.
D. Disable the data loss prevention (DLP) policy.

Answer: C

QUESTION 1778
An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

A. Intrusion detection system (IDS)
B. Security information and event management (SIEM) tool
C. File integrity monitoring (FIM) software.
D. Antivirus software

Answer: C

QUESTION 1779
An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:

A. automated reporting to stakeholders.
B. a control self-assessment process.
C. metrics for each milestone.
D. a monitoring process for the security policy.

Answer: C

QUESTION 1780
Which of the following is the FIRST step in developing a disaster recovery plan (DRP)?

A. Set a recovery point objective (RPO).
B. Perform a business impact analysis (BIA).
C. Set a recovery time objective (RTO).
D. Identify potential third-party service providers

Answer: B

QUESTION 1781
A recent comprehensive vulnerability assessment identified emerging threats to the continuity of critical business services. What should be the information security manager's FIRST course of action?

A. Conduct a gap analysis.
B. Conduct a risk assessment
C. Perform a patch update.
D. Perform a penetration test

Answer: B

QUESTION 1782
An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders^ it is MOST important to establish:

A. automated reporting to stakeholders.
B. a monitoring process for the security policy
C. a control self-assessment process
D. metrics for each milestone.

Answer: D

QUESTION 1783
Which of the following would BEST provide an information security manager with sufficient assurance that a service provider complies with organization's information security requirements?

A. A live demonstration of the third-party supplier's security capabilities
B. Third-party security control self-assessment results
C. An independent review report indicating compliance with industry standards
D. The ability to audit the third-party supplier's IT systems and processes

Answer: D

QUESTION 1784
An organization's outsourced firewall was poorly configured and allowed unauthorized access that resulted in downtime of 48 hours. Which of the following should be the information security manager's NEXT course of action?

A. Reconfigure the firewall in accordance with best practices.
B. Obtain supporting evidence that the problem has been corrected.
C. Revisit the contract and improve accountability of the service provider.
D. Seek damages from the service provider.

Answer: B

QUESTION 1785
A new information security manager finds that the organization tends to use short-term solutions to address problems. Resource allocation and spending are not effectively tracked and there is no assurance that compliance requirements are being met What should be done FIRST to reverse this bottom-up approach to security?

A. Implement an information security awareness training program
B. Create an information security steering committee
C. Conduct a threat analysis
D. Establish an audit committee

Answer: A

QUESTION 1786
A measure of the effectiveness of the incident response capabilities of an organization is the

A. reduction of the annual loss expectancy (ALE).
B. number of incidents detected.
C. number of employees receiving incident response training
D. time to closure of incidents.

Answer: B

QUESTION 1787
Which of the following is the MOST important incident management consideration for an organization subscribing to a cloud service?

A. Decision on the classification of cloud-hosted data
B. Expertise of personnel providing incident response
C. Implementation of a SIEM in the organization
D. An agreement on the definition of a security incident

Answer: D

QUESTION 1788
Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

A. Ensure that proper controls exist for code review and release management
B. Set up an agent to run a virus-scanning program across platforms
C. Implement controls for continuous monitoring of middleware transactions

D. Apply the latest patch programs to the production operating systems

Answer: A

QUESTION 1789
An organization performed a risk analysis and found a large number of assets with low-impact vulnerabilities. The NEXT action of the information security manager should be to:

A. determine appropriate countermeasures.
B. transfer the risk to a third party.
C. report to management.
D. quantify the aggregated risk.

Answer: D

QUESTION 1790
Which of the following BEST enables effective information security governance?

A. Periodic vulnerability assessments
B. Established information security metrics
C. Advanced security technologies
D. Security-aware corporate culture

Answer: B

QUESTION 1791
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

A. security requirements for the process being outsourced
B. security metrics
C. service level agreements (SLAs)
D. risk-reporting methodologies

Answer: A

QUESTION 1792
For an organization that is experiencing outages due to malicious code, which of the following is the BEST index of the effectiveness of countermeasures?

A. Number of virus infections detected
B. Amount of infection-related downtime
C. Average recovery time per incident
D. Number of downtime-related help desk calls

Answer: B

QUESTION 1793
Which of the following BEST indicates an effective vulnerability management program?

A. Controls are managed proactively.
B. Risks are managed within acceptable limits
C. Threats are identified accurately

D. Security incidents are reported in a timely manner

Answer: B

QUESTION 1794
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. Escalation paths
B. Right-to-audit clause
C. Termination language
D. Key performance indicators (KPIs)

Answer: D

QUESTION 1795
Which of the following is the MAIN benefit of performing an assessment of existing incident response processes?

A. Identification of threats and vulnerabilities
B. Prioritization of action plans
C. Validation of current capabilities
D. Benchmarking against industry peers

Answer: A

QUESTION 1796
What is the PRIMARY responsibility of the security steering committee?

A. Develop information security policy.
B. Implement information security control.
C. Set direction and monitor performance.
D. Provide information security training to employees.

Answer: C

QUESTION 1797
What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

A. Update the threat landscape
B. Review the effectiveness of controls
C. Determine operational losses
D. Improve the change control process

Answer: B

QUESTION 1798
Who should determine data access requirements for an application hosted at an organization's data center?

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

Answer: A

QUESTION 1799
Which of the following has the MOST direct impact on the usability of an organization's asset classification program?

A. The granularity of classifications in the hierarchy
B. The frequency of updates to the organization's risk register
C. The business objectives of the organization
D. The support of senior management for the classification scheme

Answer: C

QUESTION 1800
The PRIMARY goal of the eradication phase in an incident response process is to:

A. provide effective triage and containment of the incident.
B. remove the threat and restore affected systems.
C. obtain forensic evidence from the affected system.
D. maintain a strict chain of custody,

Answer: B
Explanation:
Eradication Contain the threat and restore initial systems to their initial state, or close to it. The team should isolate the root cause of the attack, remove threats and malware, and identify and mitigate vulnerabilities that were exploited to stop future attacks. These steps may change the configuration of the organization. The aim is to make changes while minimizing the effect on the operations of the organization. You can achieve this by stopping the bleeding and limiting the amount of data that is exposed.

QUESTION 1801
Which of the following would be MOST useful to help senior management understand the status of information security compliance?

A. Industry benchmarks
B. Risk assessment results
C. Business impact analysis (BIA) results
D. Key performance indicators (KPIs)

Answer: B

QUESTION 1802
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: A
Explanation:
Incident response experts are still considered local resources hired by the peer orgs. Also why would you want to go to your peers and shows them your weakness . You would want to consult with intel communities for guidance . Consultants would cost you and open source recon wouldnt be the best option due to its inherent risks .

QUESTION 1803
In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?

A. Data encryption
B. Access to the hardware
C. Compressed customer data
D. Non-standard event logs

Answer: B

QUESTION 1804
Which of the following is MOST important to consider when determining the effectiveness of the information security governance program'?

A. Key risk indicators (KRIs)
B. Key performance indicators (KPIs)
C. Maturity models
D. Risk tolerance levels

Answer: A

QUESTION 1805
Which of the following is the BEST defense against a brute force attack?

A. Discretionary access control
B. Intruder detection lockout
C. Mandatory access control
D. Time-of-day restrictions

Answer: D