Braindump2go Guarantee All Exams 100% Pass One Time!

- Vendor: Isaca
- Exam Code: CISM
- Exam Name: Certified Information Security Manager
- New Updated Questions from Braindump2go (Updated in April/2022)

Visit Braindump2go and Download Full Version CISM Exam Dumps

QUESTION 1806
To set security expectations across the enterprise, it is MOST important for the information security policy to be regularly reviewed and endorsed by

A. senior management
B. the IT steering committee.
C. the chief information security officer (CISO).
D. security administrators

Answer: B

QUESTION 1807
A large organization is in the process of developing its information security program that involves working with several complex organizational functions. Which of the following will BEST enable the successful implementation of this program?

A. Security governance
B. Security policy
C. Security metrics
D. Security guidelines

Answer: A

QUESTION 1808
Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?

A. Tabletop exercises
B. Forensics certification
C. Penetration tests
D. Disaster recovery drills

Answer: A

QUESTION 1809
Regular vulnerability scanning on an organization's internal network has identified that many user workstations have unpatched versions of software What is the BEST way for the information security manager to help senior management understand the related risk?

CISM Exam Dumps CISM Exam Questions CISM PDF Dumps CISM VCE Dumps

https://www.braindump2go.com/cism.html

A. Include the impact of the risk as part of regular metrics
B. Recommend the security steering committee conduct a review
C. Update the risk assessment at regular intervals
D. Send regular notifications directly to senior managers

Answer: A

QUESTION 1810
An organization has experienced multiple instances of privileged users misusing their access Which of the following processes would be MOST helpful in identifying such violations?

A. Review of access controls
B. Security assessment
C. Policy exception review
D. Log review

Answer: D

QUESTION 1811
Which of the following is MOST important to the successful implementation of an information security program?

A. Obtaining stakeholder input
B. Understanding current and emerging technologies
C. Conducting periodic risk assessments
D. Establishing key performance indicators (KPIs)

Answer: C

QUESTION 1812
Senior management is concerned that the incident response team took unapproved actions during incident response that put business objectives at risk. Which of the following is the BEST way (or the information security manager to respond to this situation?

A. Update roles and responsibilities of the incident response team.
B. Validate that the information security strategy maps to corporate objectives
C. Train the incident response team on escalation procedures.
D. Implement a monitoring solution for incident response activities.

Answer: D

QUESTION 1813
Which of the following is MOST important to ensuring that incident management plans are executed effectively?

A. A reputable managed security services provider has been engaged
B. The incident response team has the appropriate training
C. Management support and approval has been obtained
D. An incident response maturity assessment has been conducted

Answer: C

QUESTION 1814
What should be an information security manager's MOST important consideration when reviewing a proposed upgrade to a business unit's production database?

A. Ensuring the application inventory is updated
B. Ensuring senior management is aware of associated nsk
C. Ensuring residual risk is within appetite
D. Ensuring a cost-benefit analysis is completed

Answer: A

QUESTION 1815
A security policy exception is leading to an unexpected increase in the number of alerts about suspicious Internet traffic on an organization's network Which of the following is the BEST course of action?

A. Present a risk analysis with recommendations to senior management.
B. Update the risk register so that senior management is kept informed
C. Remove the rules that trigger the increased number of alerts
D. Evaluate and update the enterprise network security architecture

Answer: A

QUESTION 1816
Which of the following is the BEST way to determine if a recent investment in access control software was successful?

A. A comparison of security incidents before and after software installation
B. Senior management acceptance of the access control software
C. A review of the number of key risk indicators (KRIs) implemented for the software
D. A business impact analysis (BIA) of the systems protected by the software

Answer: C

QUESTION 1817
Which of the following would provide the MOST essential input for the development of an information security strategy?

A. Measurement of security performance against IT goals
B. Results of an information security gap analysis
C. Availability of capable information security resources
D. Results of a technology risk assessment

Answer: B

QUESTION 1818
An information security manager wants to improve the ability to identify changes in risk levels affecting the organization's systems. Which of the following is the BEST method to achieve this objective?

A. Performing business impact analyses (BIA)
B. Monitoring key goal indicators (KGIs)
C. Updating the risk register
D. Monitoring key risk indicators (KRIs)

Answer: A

QUESTION 1819
Senior management has just accepted the risk of noncompliance with a new regulation. What should the information security manager do NEXT?

A. Report the decision to the compliance officer.

B. Update details within the risk register
C. Reassess the organization's risk tolerance
D. Assess the impact of the regulation

Answer: B

QUESTION 1820
An organization's operations have been significantly impacted by a cyber attack resulting in data loss Once the attack has been contained, what should the security team do NEXT?

A. Conduct a lessons learned exercise.
B. Perform a root cause analysis
C. Update the incident response plan
D. Implement compensating controls.

Answer: B

QUESTION 1821
Management has announced the acquisition of a new company. The information security manager of parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies.
To BEST address this concern, the information security manager should:

A. escalate concern for conflicting access rights to management.
B. implement consistent access control standards.
C. review access rights as the acquisition integration occurs.
D. perform a risk assessment of the access rights.

Answer: D

QUESTION 1822
Which of the following should be an information security manager's MOST important cntenon for determining when to review the incident response plan?

A. When missing information impacts recovery from an incident
B. When recovery time objectives (RTOs) are not met
C. Before an internal audit of the incident response process
D. At intervals indicated by industry best practice

Answer: B

QUESTION 1823
Which of the following BEST indicates the effectiveness of the vendor risk management process?

A. Increase in the percentage of vendors certified to a globally recognized security standard
B. Increase in the percentage of vendors conducting mandatory security training
C. Increase in the percentage of vendors that have reported secunty breaches
D. Increase in the percentage of vendors with a completed due diligence review

Answer: C

QUESTION 1824
Which of the following is the BEST way to strengthen the security of corporate data on a personal mobile device?

A. Implementing a strong password policy
B. Using containerized software
C. Mandating use of pre-approved devices
D. implementing multi-factor authentication

Answer: C

QUESTION 1825
Which of the following is the BEST way to enhance training for incident response teams?

A. Conduct interviews with organizational units
B. Participate in emergency response activities
C. Perform post-incident reviews
D. Establish incident key performance indicators (KPIs).

Answer: B

QUESTION 1826
Which of the following should an information security manager do FIRST after a new cybersecurity regulation has been introduced?

A. Update the information security policy
B. Consult corporate legal counsel
C. Perform a gap analysis
D. Conduct a cost-benefit analysis.

Answer: C

QUESTION 1827
An organization has fallen victim to a spear-phishing attack that compromised the multi-factor authentication code. What is the information security manager's MOST important follow-up action?

A. Install client anti-malware solutions
B. Communicate the threat to users.
C. Implement an advanced email filtering system.
D. Implement firewall blocking of known attack signatures.

Answer: B

QUESTION 1828
Which of the following is the MOST important consideration when reporting the effectiveness of an information security program to key business stakeholders"

A. Demonstrating a decrease in information security incidents
B. Linking security metrics to business objectives
C. Linking security metrics to the business impact analysis (BIA)
D. Demonstrating cost savings of each control

Answer: B

QUESTION 1829
The BEST indication of a change in risk that may negatively impact an organization is an increase

A. security incidents reported by staff to the information security team.

B. alerts triggered by the security information and event management (SIEM) solution.
C. events logged by the intrusion detection system (IDS).
D. malware infections detected by the organization's anti-virus software.

Answer: A

QUESTION 1830
Which of the following is the MAIN objective of a risk management program?

A. Reduce costs associated with incident response.
B. Reduce risk to the maximum extent possible.
C. Reduce risk to the level of the organization's risk appetite.
D. Reduce corporate liability for information security incidents.

Answer: C

QUESTION 1831
Which of the following is MOST appropriate to communicate to senior management regarding information risk?

A. Emerging security technologies
B. Risk profile changes
C. Defined risk appetite
D. Vulnerability scanning progress

Answer: D

QUESTION 1832
Which of the following is the BEST way to evaluate the impact of threat events on an organization's IT operations?

A. Controls review
B. Penetration testing
C. Risk assessment
D. Scenario analysis

Answer: D

QUESTION 1833
A new regulatory requirement affecting an organization's information security program is released.
Which of the following should be the information security manager's FIRST course of action?

A. Conduct benchmarking.
B. Determine the disruption to the business.
C. Perform a gap analysis.
D. Notify the legal department.

Answer: C

QUESTION 1834
Which of the following should be the PRIMARY driver for selecting and implementing appropriate controls to address the risk associated with weal user passwords?

A. The cost of risk mitigation controls
B. The organization's risk tolerance
C. The organization's culture

D. Direction from senior management

Answer: A

QUESTION 1835
To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?

A. Level of residual risk
B. Configuration parameters
C. Gap analysis results
D. Level of risk treatment

Answer: A

QUESTION 1836
In information security manager MUST have an understanding of the organization's business goals to:

A. define key performance indicators (KPIs).
B. develop an information security strategy.
C. develop operational procedures.
D. relate information security to change management.

Answer: C

QUESTION 1837
An information security manager needs to ensure security testing is conducted on a new system.
Which of the following would provide the HIGHEST level of assurance?

A. The vendor provides the results of a penetration test and code review.
B. An independent party is directly engaged to conduct testing.
C. The security team conducts a self-assessment against a recognized industry framework.
D. The internal audit team is enlisted to run a vulnerability assessment against the system.

Answer: B

QUESTION 1838
Which of the following should be the PRIMARY driver for delaying the delivery of an information security awareness program?

A. Risk appetite
B. Change in senior management
C. High employee turnover
D. Employee acceptance

Answer: A

QUESTION 1839
Which of the following would MOST effectively communicate the benefits of an information security program to executive management?

A. Industry benchmarks
B. Key performance indicators (KPIs)
C. Threat models

D. Key risk indicators (KRIs)

Answer: D

QUESTION 1840
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server. Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

A. A continual server replication process
B. Employee training on ransomware
C. A properly configured firewall
D. A properly tested offline backup system

Answer: D

QUESTION 1841
When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:

A. challenge the incident response team to solve the problem under pressure.
B. give the business a measure of the organization's overall readiness.
C. measure management engagement as part of an incident response team.
D. provide participants with situations to ensure understanding of their roles.

Answer: D

QUESTION 1842
Audit trails of changes to source code and object code are BEST tracked through:

A. job control statements.
B. code review.
C. use of compilers.
D. program library software.

Answer: D

QUESTION 1843
Which of the following is MOST important to include when reporting information security risk to executive leadership?

A. Key performance objectives and budget trends
B. Security awareness training participation and residual risk exposures
C. Risk analysis results and key risk indicators (KRIs)
D. Information security risk management plans and control compliance

Answer: C

QUESTION 1844
Which of the following is MOST important to include in an information security status report to senior management?

A. Key risk indicators (KRIs)
B. Review of information security policies
C. List of recent security events
D. Information security budget requests

Answer: A

QUESTION 1845
An organization finds unauthorized software has been installed on a number of workstations. The software was found to contain a Trojan, which had been uploading data to an unknown external party. Which of the following would have BEST prevented the installation of the unauthorized software?

A. Banning executable file downloads at the Internet firewall
B. Implementing application blacklisting
C. Removing local administrator rights
D. Implementing an intrusion detection system (IDS)

Answer: C

QUESTION 1846
Which of the following is MOST likely to affect an organization's ability to respond to security incidents in a timely manner?

A. Inadequate detective control performance
B. Lack of senior management buy-in
C. Complexity of network segmentation
D. Misconfiguration of security information and event management (SIEM) tool

Answer: D

QUESTION 1847
Which of the following will protect the confidentiality of data transmitted over the Internet?

A. Network address translation
B. Message digests
C. Encrypting file system
D. IPsec protocol

Answer: D

QUESTION 1848
When establishing metrics for an information security program, the BEST approach is to identify indicators that:

A. demonstrate the effectiveness of the security program.
B. reduce information security program spending.
C. reflect the corporate risk culture.
D. support major information security initiatives.

Answer: A

QUESTION 1849
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

A. Right of the subscriber to conduct onsite audits of the vendor
B. Escrow of software code with conditions for code release
C. Commingling of subscribers' data on the same physical server
D. Authority of the subscriber to approve access to its data

Answer: A

QUESTION 1850
Which of the following is the MOST relevant factor when determining the appropriate escalation process in the incident response plan?

A. Replacement cost of the affected systems
B. Resilience capability of the affected systems
C. Significance of the affected systems
D. Number of resources allocated to respond

Answer: C

QUESTION 1851
Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?

A. Monitor the effectiveness of controls.
B. Review the risk probability and impact.
C. Review the inherent risk level.
D. Update the risk assessment framework.

Answer: A

QUESTION 1852
Which of the following information BEST supports risk management decision making?

A. Average cost of risk events
B. Results of a vulnerability assessment
C. Estimated savings resulting from reduced risk exposure
D. Quantification of threats through threat modeling

Answer: C

QUESTION 1853
Which of the following roles is BEST suited to validate user access requirements during an annual user access review?

A. System administrator
B. Access manager
C. Business owner
D. IT director

Answer: C

QUESTION 1854
Which of the following is the MOST relevant information to include in an information security risk report to facilitate senior management's understanding of impact to the organization?

A. Detailed assessment of the security risk profile
B. Risks inherent in new security technologies
C. Status of identified key security risks
D. Findings from recent penetration testing

Answer: C

QUESTION 1855
A recent audit found that an organization's new user accounts are not set up uniformly. Which of the following is MOST important for the information security manager to review?

A. Guidelines
B. Automated controls
C. Standards
D. Security policies

Answer: C

QUESTION 1856
An information security manager has become aware that a third-party provider is not in compliance with the statement of work (SOW). Which of the following is the BEST course of action?

A. Assess the extent of the issue.
B. Initiate contract renegotiation.
C. Notify senior management of the issue.
D. Report the issue to legal personnel.

Answer: A

QUESTION 1857
Which of the following is MOST likely to be a component of a security incident escalation policy?

A. Sample scripts and press releases for statements to media
B. Names and telephone numbers of key management personnel
C. Decision criteria for when to alert various groups
D. A severity-ranking mechanism tied only to the duration of the outage

Answer: D

QUESTION 1858
For an enterprise implementing a bring your own device (BYOD) program, which of the following would provide the BEST security of corporate data residing on unsecured mobile devices?

A. Acceptable use policy
B. Data loss prevention (DLP)
C. Device certification process
D. Containerization solution

Answer: D

QUESTION 1859
Which of the following should be the MOST important consideration when reviewing an information security strategy?

A. New business initiatives
B. Changes to the security budget
C. Recent security incidents
D. Internal audit findings

Answer: B

QUESTION 1860

Application data integrity risk is MOST directly addressed by a design that includes:

A. application log requirements such as field-level audit trails and user activity logs.
B. strict application of an authorized data dictionary.
C. access control technologies such as role-based entitlements.
D. reconciliation routines such as checksums, hash totals, and record counts.

Answer: C

QUESTION 1861
Which of the following is the PRIMARY objective of defining a severity hierarchy for security incidents?

A. To facilitate the classification of an organization's IT assets
B. To streamline the risk analysis process
C. To prioritize available incident response resources
D. To facilitate root cause analysis of incidents

Answer: C

QUESTION 1862
Which of the following is the MOST effective way for an organization to ensure its third-party service providers are aware of information security requirements and expectations?

A. Providing information security training to third-party personnel
B. Including information security clauses within contracts
C. Requiring third parties to sign confidentiality agreements
D. Auditing the service delivery of third-party providers

Answer: B

QUESTION 1863
The GREATEST benefit resulting from well-documented information security procedures is that they:

A. provide a basis for auditing security practices.
B. facilitate security training of new staff.
C. ensure processes can be followed by temporary staff.
D. ensure that security policies are consistently applied.

Answer: D

QUESTION 1864
Which of the following is the MOST effective approach for determining whether an organization's information security program supports the information security strategy?

A. Develop key performance indicators (KPIs) of information security.
B. Ensure resources meet information security program needs.
C. Identify gaps impacting information security strategy.
D. Audit the information security program to identify deficiencies.

Answer: A

QUESTION 1865
Which of the following is the MOST essential element of an information security program?

A. Benchmarking the program with global standards for relevance
B. Applying project management practices used by the business
C. Prioritizing program deliverables based on available resources
D. Involving functional managers in program development

Answer: D

QUESTION 1866
Which of the following should an information security manager do FIRST when a legacy application is not compliant with a regulatory requirement, but the business unit does not have the budget for remediation?

A. Notify legal and internal audit of the noncompliant legacy application.
B. Develop a business case for funding remediation efforts.
C. Advise senior management to accept the risk of noncompliance.
D. Assess the consequences of noncompliance against the cost of remediation.

Answer: D

QUESTION 1867
An information security manager has identified that security risks are not being treated in a timely manner. Which of the following is the BEST way to address this situation?

A. Provide regular updates about the current state of the risks.
B. Create mitigating controls to manage the risks.
C. Re-perform risk analysis at regular intervals.
D. Assign a risk owner to each risk.

Answer: D

QUESTION 1868
An information security manager notes that security incidents are not being appropriately escalated by the help desk after tickets are logged. Which of the following is the BEST automated control to resolve this issue?

A. Integrating automated service level agreement (SLA) reporting into the help desk ticketing system
B. Changing the default setting for all security incidents to the highest priority
C. Implementing automated vulnerability scanning in the help desk workflow
D. Integrating incident response workflow into the help desk

Answer: D

QUESTION 1869
Which of the following BEST demonstrates that an anti-phishing campaign is effective?

A. Improved feedback on the anti-phishing campaign
B. Decreased number of incidents that have occurred
C. Improved staff attendance in awareness sessions
D. Decreased number of phishing emails received

Answer: B

QUESTION 1870
Which of the following is the MOST important element in the evaluation of inherent security risks?

A. Impact to the organization

B. Cast of countermeasures
C. Control effectiveness
D. Residual risk

Answer: A

QUESTION 1871
Which of the following components of an information security risk assessment is MOST valuable to senior management?

A. Return on investment (ROI)
B. Mitigation actions
C. Residual risk
D. Threat profile

Answer: C

QUESTION 1872
The PRIMARY benefit of a centralized time server ts that it

A. allows decentralized logs to be kept in synchronization.
B. reduces individual time-of-day requests by client applications,
C. 15 required by password synchronization programs.
D. decreases the likelihood of an unrecoverable systems failure.

Answer: A

QUESTION 1873
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A. obtain the support of executive management
B. document the disaster recovery process.
C. map the business process to supporting IT and other corporate resources
D. identify critical processes and the degree of reliance on support services.

Answer: D

QUESTION 1874
Which of the following is the MOST important security feature an information security manager would need for a mobile device management (MDM) program?

A. Ability to inventory devices
B. Ability to remotely wipe devices
C. Ability to locate devices
D. Ability to push updates to devices

Answer: A

QUESTION 1875
The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:

A. the steering committee.

B. the board of directors.
C. the internal audit manager.
D. the information security officer,

Answer: B

QUESTION 1876
Which of the following is the BEST way for an organization to determine the maturity level of its information security program?

A. Review the results of information security awareness testing
B. Track the trending of information security incidents.
C. Validate the effectiveness of implemented security controls.
D. Benchmark the information security policy against industry standards.

Answer: C

QUESTION 1877
Senior management has launched an enterprise-wide initiative to streamline internal processes to reduce costs, including security processes. What should the information security manager rely on MOST to allocate resources efficiently?

A. Return on investment (ROI)
B. Risk classification
C. Capability maturity assessment
D. Internal audit reports

Answer: B

QUESTION 1878
Which of the following is the PRIMARY responsibility of an information security steering committee composed of management representation from business units?

A. Perform business impact analyses (BIAS).
B. Monitor the treatment of information security risk.
C. Oversee the execution of the information security strategy
D. Manage the implementation of the information security plan.

Answer: C

QUESTION 1879
An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?

A. Conduct a risk assessment.
B. Initiate a device reset.
C. Disable remote access,
D. Initiate incident response.

Answer: D

QUESTION 1880
A corporate information security program is BEST positioned for success when:

A. the program aligns with industry best practice.
B. senior management supports the program.
C. security is thoroughly assessed in the program.
D. Staff is receptive to the program.

Answer: B

QUESTION 1881
Which of the following processes can be used to remediate identified technical vulnerabilities?

A. Enforcing baseline configurations
B. Updating the business impact analysis (BIA)
C. Conducting a risk assessment
D. Performing penetration testing

Answer: B

QUESTION 1882
Organization A offers e-commerce services and uses secure transport protacal to protect Internet communication. To confirm communication with Organization A, which of the following would be the BEST for a client to verify?

A. The URL of the 6-commerce server
B. The certificate of the e-commerce server
C. The browser's indication of SSL use
D. The IP address of the e-commerce server

Answer: B

QUESTION 1883
An organization's IT department needs to implement security patches. Recent reports indicate these patches could result in stability issues. Which of the following is the information security manager's BEST recommendation?

A. Research compensating security controls.
B. Research alternative software solutions,
C. Evaluate the patches in a test environment.
D. Increase monitoring after patch implementation.

Answer: C

QUESTION 1884
An information security team plans to increase password complexity requirements for a customer- facing site, but there are concerns it will negatively impact the user experience. Which of the following is the information security manager's BEST course of action?

A. Assess business impact against security risk.
B. Evaluate business compensating controls.
C. Conduct industry benchmarking.
D. Quantify the security risk to the business.

Answer: A

QUESTION 1885
Which of the following is a PRIMARY responsibility of the information security governance function?

A. Defining security strategies to support organizational programs
B. Administering information security awareness training
C. Ensuring adequate support for solutions using emerging technologies
D. Advising senior management on optimal levels of risk appetite and tolerance

Answer: A

QUESTION 1886
Which of the following BEST determines what information should be shared with different entities during incident response?

A. Disaster recovery policy
B. Communication plan
C. Business continuity plan (BCP)
D. Escalation procedures

Answer: B

QUESTION 1887
Which of the following is the PRIMARY reason that an information security manager would contract with an external provider to perform penetration testing?

A. To mitigate gaps in technical skills
B. To obtain an independent view of vulnerabilities
C. To obtain the full list of system vulnerabilities
D. To obtain an independent network security certification

Answer: A

QUESTION 1888
Which of the following is MOST important to consider when determining the criticality and sensitivity of an information asset?

A. Business functions supported by the asset
B. Number of threats that can impact the asset
C. Results of business continuity testing
D. Investment required to protect the asset

Answer: A

QUESTION 1889
Which is the MOST important requirement when establishing a process for responding to zero-day vulnerabilities?

A. Business users stop using the impacted application until a patch is released.
B. The information security team implements recommended workarounds.
C. The IT team implements an emergency patch deployment process.
D. The IT team updates antivirus signatures on user systems.

Answer: B

QUESTION 1890
The PRIMARY advantage of single sign-on (SSO) is that it will:

A. increase the security of related applications.

B. support multiple authentication mechanisms.
C. increase efficiency of access management.
D. strengthen user passwords.

Answer: C

QUESTION 1891
Which of the following would provide the MOST useful information when prioritizing controls to be added to a system?

A. Baseline to industry standards
B. The risk register
C. Balanced scorecard
D. Compliance requirements

Answer: B

QUESTION 1892
An organization has recently acquired a smaller company located in a different geographic region.
Which of the following is the BEST approach for addressing conflicts between the parent organization's security standards and local regulations affecting the acquired company?

A. Adopt the standards of the newly acquired company.
B. Give precedence to the parent organization's standards.
C. Create a global version of the local regulations,
D. Create a local version of the parent organization's standards.

Answer: B

QUESTION 1893
An organization has decided to outsource its disaster recovery function. Which of the following is the MOST important consideration when drafting the service level agreement (SLA)?

A. Recovery time objectives (RTOs)
B. Testing requirements
C. Recovery point objectives (RPOs)
D. Authorization chain

Answer: B

QUESTION 1894
Which of the following MOST effectively allows for disaster recovery testing without interrupting business operations?

A. Full interruption testing
B. Simulation testing
C. Parallel testing
D. Structured walk-through

Answer: A

QUESTION 1895
When defining and communicating roles and responsibilities between an organization and cloud service provider, which of the following situations would present the GREATEST risk to the organization's ability to ensure information risk is managed appropriately?

A. The Service agreement results in unnecessary duplication of effort because shared responsibilities have not been clearly defined.
B. The organization and provider identified multiple information security responsibilities that neither party was planning to provide.
C. The service agreement uses a custom-developed RACI instead of an industry standard RACI to document responsibilities.
D. The organization believes the provider accepted responsibility for issues affecting security that the provider did not accept.

Answer: D

QUESTION 1896
An organization has implemented a new security control in response to a recently discovered vulnerability. Several employees have voiced concerns that the control disrupts their ability to work. Which of the following is the information security manager's BEST course of action?

A. Educate users about the vulnerability.
B. Report the control risk to senior management.
C. Accept the vulnerability.
D. Evaluate compensating control options.

Answer: D

QUESTION 1897
An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resalve the issue, it took a significant amount of time to identify, What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Implement a SIEM solution.
B. Perform a post-incident review.
C. Perform a threat analysis.
D. Establish performance metrics for the team.

Answer: B

QUESTION 1898
An organization's ClO has tasked the information security manager with drafting the charter for an information security steering committee. The committee will be comprised of the C/O, the IT shared services manager, the vice president of marketing, and the information security manager. Which of the following is the MOST significant issue with the development of this committee?

A. The CIO is not taking charge of the committee.
B. There is a conflict of interest between the business and IT.
C. The committee lacks sufficient business representation.
D. The committee consists of too many senior executives.

Answer: C

QUESTION 1899
Which of the following is MOST important to ensure when considering exceptions to an information security policy?

A. Exceptions are based on data classification.
B. Exceptions undergo regular review.
C. Exceptions reflect the organizational risk appetite.

D. Exceptions are approved by executive management.

Answer: C

QUESTION 1900
Which of the following would be MOST useful in determining how an organization will be affected by a new regulatory requirement for cloud services?

A. Risk assessment
B. Data classification policy
C. Information asset inventory
D. Data loss protection plan

Answer: A

QUESTION 1901
Which of the following is an information security manager's BEST course of action upon discovering an organization with budget constraints lacks several important security capabilities?

A. Suggest the deployment of open-source security tools to mitigate identified risks.
B. Recommend that the organization avoid the most severe risks.
C. Establish a business case to demonstrate return on investment (ROI) of a security tool.
D. Review the most recent audit report and request funding to address the most serious finding.

Answer: C

QUESTION 1902
Which of the following is the BEST way to strengthen the alignment of an information security program with business strategy?

A. Providing organizational training on information security policies
B. Increasing budget for risk assessments
C. Increasing the frequency of control assessments
D. Establishing an information security steering committee

Answer: D

QUESTION 1903
Which of the following is the PRIMARY responsibility of an information security governance committee?

A. Approving changes to the information security strategy
B. Discussing upcoming information security projects
C. Reviewing monthly information security metrics
D. Reviewing the information security risk register

Answer: A

QUESTION 1904
An organization has established a bring your own device (BYOD) program. Which of the following is the MOST important security consideration when allowing employees to use personal devices for corporate applications remotely?

A. Security awareness training
B. Secure application development
C. Mobile operating systems support

D. Mandatory controls for maintaining security policy

Answer: A

QUESTION 1905
An organization is developing a disaster recovery strategy and needs to identify each application's criticality so that the recovery sequence can be established. Which of the following is the BEST course of action?

A. Document the data flow and review the dependencies.
B. Perform a business impact analysis (BIA) on each application.
C. Restore the applications with the shortest recovery times first.
D. Identify which applications contribute the most cash flow.

Answer: B

QUESTION 1906
an information security manager has identified a major security event with potential noncompliance implications. Who should be notified FIRST?

A. Internal audit
B. Senior management
C. Public relations team
D. Regulatory authorities

Answer: B

QUESTION 1907
Which of the following should be the PRIMARY focus of a status report on the information security program to senior management?

A. Demonstrating risk is managed at the desired level
B. Confirming the organization complies with security policies
C. Providing evidence that resources are performing as expected
D. Verifying security costs do not exceed the budget

Answer: A

QUESTION 1908
To address the issue that performance pressures on IT may conflict with information security controls, itis MOST important that:

A. the Steering committee provides guidance and dispute resolution.
B. noncompliance issues are reported to senior management.
C. IT policies and procedures are better aligned to security policies.
D. the security policy is changed to accommodate IT performance pressure.

Answer: A

QUESTION 1909
Which of the following would BEST help an organization's ability to manage advanced persistent threats (APT)?

A. Using multiple security vendors
B. Having a skilled information security team
C. Having network detection tools in place

D. Increasing the information security budget

Answer: C

QUESTION 1910
Priore implementing a bring your own device (BYOD) program, it is MOST important to:

A. select mobile device management (MDM) software.
B. survey employees for requested applications.
C. review currently utilized applications.
D. develop an acceptable use policy.

Answer: D

QUESTION 1911
In an organization that has several independent security tools including intrusion detection systems (IDSs) and firewalls, which of the following is the BEST way to ensure timely detection of incidents?

A. Ensure staff are cross trained to manage all security tools.
B. Ensure that the incident response plan is endorsed by senior management.
C. Outsource the management of security tools to a service provider.
D. Implement a log aggregation and correlation solution.

Answer: D

QUESTION 1912
Which of the following is the PRIMARY responsibility of an information security steering committee?

A. Revigwing firewall rules
B. Setting up password expiration procedures
C. Prioritizing security initiatives
D. Drafting security policies

Answer: C

QUESTION 1913
Which of the following would be MOST helpful when determining appropriate access controls for an application?

A. End-user input
B. Industry best practices
C. Data criticality
D. Gap analysis results

Answer: C

QUESTION 1914
Which of the following provides the MOST relevant information to determine the overall effectiveness of an information security program and underlying business processes?

A. SWOT analysis
B. Balanced scorecard
C. Cost-benefit analysis
D. Industry benchmarks

Answer: B

QUESTION 1915
What should be an information security manager's MOST important consideration when reviewing a proposed upgrade to a business unit's production database?

A. Ensuring residual risk is within apbetite
B. Ensuring the application inventory is updated
C. Ensuring a cost-benefit analysis is completed
D. Ensuring senior management is aware of associated risk

Answer: A

QUESTION 1916
Which of the following metrics provides the BEST measurement of the effectiveness of a security awareness program?

A. Mean time between incident detection and remediation
B. Variance of program cost to allocated budget
C. The number of reported security incidents
D. The number of security breaches

Answer: A

QUESTION 1917
Which of the following is an information security manager's FIRST priority after a high-profile system has been compromised?

A. Implement improvements to prevent recurrence.
B. Identify the malware that compromised the system.
C. Preserve incident-related data.
D. Restore the compromised system.

Answer: D

QUESTION 1918
Which of the following should an information security manager do FIRST to address complaints that a newly implemented security control has slowed business operations?

A. Discuss the issue with senior management for direction.
B. Validate whether the control is operating as intended.
C. Remove the control and identify alternatives.
D. Conduct user awareness training.

Answer: B

QUESTION 1919
An information security manager was informed that a planned penetration test could potentially disrupt some services. Which of the following should be the FIRST course of action?

A. Ensure the service owner is available during the penetration test.
B. Accept the risk and document it in the risk register.
C. Estimate the impact and inform the business owner.
D. Reschedule the activity during an approved maintenance window.

Answer: C

QUESTION 1920
What is the PRIMARY objective of implementing standard security configurations?

A. Maintain a flexible approach to mitigate potential risk to unsupported systems.
B. Compare configurations between supported and unsupported systems.
C. Minimize the operational burden of managing and monitoring unsupported systems.
D. Control vulnerabilities and reduce threats from changed configurations.

Answer: D

QUESTION 1921
In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?

A. Allocation of training resources
B. Compliance with policies
C. Auditability of systems
D. Ownership of security

Answer: D

QUESTION 1922
When developing an incident escalation process, the BEST approach is to classify incidents based on:

A. estimated time to recover.
B. information assets affected.
C. their root causes.
D. recovery point objectives (RPOs).

Answer: D

QUESTION 1923
An employee clicked on a link in a phishing email, triggering a ransomware attack. Which of the following should be the information security manager's FIRST step?

A. Wipe the affected system.
B. lsolate the impacted endpoints.
C. Notify senior management
D. Notify internal legal counsel.

Answer: B

QUESTION 1924
The PRIMARY purpose for defining key risk indicators (KRIs) for a security program is to:

A. ensure mitigating controls meet specifications.
B. provide information needed to take action.
C. support investments in the security program.
D. compare security program effectiveness to benchmarks.

Answer: A

QUESTION 1925
An information security manager is preparing incident response plans for an organization that processes personal and financial information. Which of the Following is the MOST important consideration?

A. Identifying regulatory requirements
B. Determining budgetary constraints.
C. Aligning with enterprise architecture (EA)
D. Aligning with an established industry framework

Answer: A

QUESTION 1926
To implement effective continuous monitoring of IT controls, an information security manager needs to FIRST ensure:

A. security alerts are centralized.
B. periodic scanning of IT systems is in place.
C. metrics are communicated to senior management.
D. information assets have been classified.

Answer: C

QUESTION 1927
Which of the following is MOST likely to be included in an enterprise security policy?

A. Retention schedules
B. Organizational risk
C. System access specifications
D. Definitions of responsibilities

Answer: D

QUESTION 1928
Which of the following is the BEST way to build a risk-aware culture?

A. Periodically test compliance with security controls and post results.
B. Periodically change risk awareness messages.
C. Ensure that threats are communicated organization-wide in a timely manner.
D. Establish incentives and a channel for staff to report risks.

Answer: A