ISACA.CISM.v2020-10-29.q287

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	287
Version:	v2020-10-29
# of views:	1757
# of Questions views:	75893
https://www.freecram.net/torrent/ISACA.CISM.v2020-10-29.q287.html	

NEW QUESTION: 1
The PRIMARY advantage of a network intrusion detection system (IDS) is that it can:
A. identify an attack on the network.
B. simulate denial-of-service attacks.
C. detect network vulnerabilities
D. block undesirable network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following is MOST important to include in an information security strategy?
A. Current and future desired state of information security
B. Information security organizational structures and responsibilities
C. Cost reduction techniques for information security investments
D. Information security program needs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
An incident was detected where customer records were altered without authorization. The GREATEST concern for forensic analysis would be that the log data:
A. may be modified.
B. has been disclosed.
C. could be temporarily available.
D. may not be time-synchronized.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4

Which of the following would provide senior management with the BEST information to better understand the organization's information security risk profile?
A. Scenarios that impact business goals
B. Scenarios that impact business operations
C. Scenarios that disrupt client services
D. Scenarios that have a monetary impact
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following provides the MOST relevant evidence of incident response maturity?
A. Red team testing results
B. Average incident closure time
C. Independent audit assessment
D. Tabletop exercise results
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which of the following is the MOST important reason for performing a risk analysis?
A. Identifying critical information assets
B. Identifying and eliminating threats
C. Promoting increased security awareness in the organization
D. Assigning the appropriate level of protection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
Implementing a strong password policy is part of an organization s information security strategy for the year.
A business unit believes the strategy may adversely affect a client's adoption of a recently developed mobile application and has decided not to implement the policy. Which of the following is the information security manager s BEST course of action?
A. Develop and implement a password policy for d mobile application
B. Benchmark with similar mobile applications to identify gaps
C. Escalate non-implementation of the policy to senior management
D. Analyze the risk and impact of not implementing the policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which of the following is the GREATEST benefit of integrating a security information and event management (SIEM) solution with traditional security tools such as IDS, anti-malware. and email screening solutions?
A. A reduction in operational costs

B. An increase in visibility into patterns of potential threats
C. The consolidation of tools into a single console
D. The elimination of false positive detections
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following should be the information security manager's NEXT step following senior management approval of the information security strategy?
A. Develop a security pokey.
B. Form a steering committee
C. Develop a budget
D. Perform a gap analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following is MOST helpful to management in determining whether risks are within an organization's tolerance level?

A. Maturity level
B. Audit findings
C. Heat map
D. Penetration test results
Answer: (SHOW ANSWER)

NEW QUESTION: 11
A security incident has resulted in a failure of the enterprise resource planning (ERP) system. While the incident is handled by the incident response team, the help desk is overrun by queries from department managers on the state of the ERP system. What is the MOST likely reason for this situation?
A. An inadequate business impact analysis (BIA)
B. Lack of organization-wide security awareness
C. Lack of knowledgeable help desk staff
D. An inadequate communication plan
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following BEST describes a buffer overflow?
A. A function is carried out with more data than the function can handle.
B. A program contains a hidden and unintended function that presents a security risk.
C. Malicious code designed to interfere with normal operations.
D. A type of covert channel that captures data.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following should an incident response team do NEXT after validating an event is an incident?
A. Escalate to management
B. Invoke the response plan.
C. Identify the toot cause.
D. Contain the incident.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
An information security manager has identified and implemented mitigating controls according to industry best practices. Which of the following is the GREATEST risk associated with this approach?
A. The mitigation measures may not be updated in a timely manner.
B. The cost of control implementation may be too high.
C. The security program may not be aligned with organizational objectives.
D. Important security controls may be missed without senior management input.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following is the MOST important component of a risk profile?
A. Data classification results
B. Risk management framework
C. Risk assessment methodology
D. Penetration test results
Answer: (SHOW ANSWER)

NEW QUESTION: 16
An organization is considering whether to allow employees to use personal computing devices for business purposes To BEST facilitate senior management's decision, the information security manager should:
A. map the strategy to business objectives.
D, perform a cost-benefit analysis.
B. develop a business case.
C. conduct a risk assessment.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
An application system stores customer confidential data and encryption is not practical. The BEST measure to protect against data disclosure is:
A. nondisclosure agreements (NDA).
B. single sign-on.
C. multi-factor access controls.
D. regular review of access logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which of the following would BEST justify spending for a compensating control?
A. Vulnerability analysis
B. Peer benchmarking
C. Threats analysis
D. Risk analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following is the MOST important reason to document information security incidents that are reported across the organization?
A. Evaluate the security posture of the organization.
B. Identify unmitigated risk.
C. Prevent incident recurrence.
D. Support business investments in security
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following BEST demonstrates effective information security management within an organization?

A. Control ownership is assigned to parties who can accept losses related to control failure.
B. Information security governance is incorporated into organizational governance.
C. Employees support decisions made by information security management.
D. Excessive risk exposure in one department can be absorbed by other departments.

Answer: (SHOW ANSWER)

NEW QUESTION: 21
A recent audit has identified that security controls required 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 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: (SHOW ANSWER)

NEW QUESTION: 22
Which of the following is an information security manager's BEST course of action when informed of decision to reduce funding for the information security program?
A. Remove overlapping security controls
B. Design key risk indicators (KRIs)
C. Prioritize security projects based on risk.
D. Create a business case appeal decision.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
When reporting to senior management on an information security vulnerability that could lead to a potential breach, what information is MOST likely to facilitate the decision-making process?
A. Business impact
B. Risk treatment options
C. Cost to remediate
D. Regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 24
An information security manager learns users of an application are frequently using emergency elevated access privileges to process transactions Which of the following should be done FIRST?
A. Review the security architecture of the application and recommend changes
B. Request justification from the users managers for emergence access
C. Update the frequency and usage of the emergency access profile in the policy
D. Request the application administrator block all emergency access profiles.
Answer: (SHOW ANSWER)

NEW QUESTION: 25

Which of the following is MOST important for an information security manager to highlight when presenting the organization s security posture to an executive audience?
A. Published sophisticated security threats targeting the Industry
B. Performance metrics specific to business urn! security awareness training
C. Security risks that may inhibit business objectives
D. The number of emails blocked by the data loss prevention (DLP) system
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which of the following would BEST ensure that application security standards are in place?
A. Functional testing
B. Penetration testing
C. Performing a code review
D. Publishing software coding standards
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
Which of the following provides the BEST evidence that a recently established information security program is effective?
A. The number of reported incidents has increased
B. The number of tickets associated with IT incidents have stayed consistent
C. Regular IT balanced scorecards are communicated
D. Senior management has reported fewer junk emails
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following metrics is the BEST measure of the effectiveness of an information security program?
A. Reduction In the number of vulnerabilities in an organization
B. Reduction In the cost of risk remediation for an organization
C. Reduction in the amount of risk exposure man organ nation
D. Reduction in the number of threats to an organization
Answer: (SHOW ANSWER)

NEW QUESTION: 29
An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?
A. Assess the consequences of noncompliance,
B. Revise the organization s security policy
C. Document risk acceptances.
D. Conduct an information security audit

Answer: (SHOW ANSWER)

NEW QUESTION: 30

Which of the following would MOST likely require a business continuity plan to be invoked'

A. A distributed denial of service attack on an email server

B. An unauthorized visitor discovered in the data center

C. An epidemic preventing staff from performing job functions

D. A hacker holding personally identifiable information hostage

Answer: (SHOW ANSWER)

NEW QUESTION: 31

During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

A. Identification

B. Eradication

C. Review

D. Containment

Answer: (SHOW ANSWER)

NEW QUESTION: 32

Which of the following is a MAIN security challenge when conducting a post-incident review related to bring your own device (BYOD) in a mature, diverse organization?

A. Ability to obtain possession of devices

B. Diversity of operating systems

C. Lack of mobile forensics expertise

D. Ability to access devices remotely

Answer: (SHOW ANSWER)

NEW QUESTION: 33

The MAIN reason for internal certification of web-based business applications is to ensure:

A. changes to the organizational policy framework are identified,

B. compliance with organizational policies.

C. up-to-date web technology is being used.
D. compliance with industry standards-
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Reviewing security objectives and ensuring the integration of security across business units is PRIMARILY the focus of the:
A. board of directors.
B. executive management
C. chief information security officer (CISO).
D. steering committee.
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which of the following would be an information security manager's BEST course of action upon learning a third-party cloud provider is not meeting information security with regard to data encryption?
A. Recommend compensating controls to mitigate the risk.
B. Report the risk to relevant stakeholders.
C. Provide a date of remediation to the cloud provider.
D. Discontinue engagement with the cloud provider.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which of the following BEST facilitates the development of a comprehensive information security policy?
A. An established internal audit program
B. An adequately funded information security budget
C. Key performance indicators (KPIs)
D. References to known industry standards
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following BEST indicates that information security will be considered when new IT technologies are implemented across an organization?
A. The information security function reports to the chief information officer.
B. Employees receive information security awareness training.
C. IT employee job descriptions include information security roles and responsibilities.
D. The information security manager is on the IT architecture review board.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
The BEST way to minimize errors in the response to an incident is to:
A. analyze the situation during the incident.
B. follow standard operating procedures.
C. reference system administration manuals.
D. implement vendor recommendations.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following is MOST useful to include in a report to senior management on a regular basis to demonstrate the effectiveness of the information security program?
A. Key performance indicators (KPIs)
B. Critical success factors (CSFs)
C. Key risk indicators (KRIs)
D. Capability maturity models
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following is the MOST important reason to consider the role of the IT service desk when developing incident handling procedures?

A. Untrained service desk personnel may be a cause of security incidents.
B. The service desk provides information to prioritize systems recovery based on user demand
C. The service desk provides a source for the identification of security incidents.
D. Service desk personnel have information on how to resolve common systems issues
Answer: (SHOW ANSWER)

NEW QUESTION: 41
After logging in to a web application, additional authentication is required at various application points. Which of the following is the PRIMARY reason for such an approach?
A. To support strong two-factor authentication protocols
B. To implement a challenge response test
C. To ensure access rights meet classification requirements
D. To meet single sign-on authentication standards
Answer: (SHOW ANSWER)

NEW QUESTION: 42
An organization has announced new initiatives to establish a big data platform and develop mobile apps. What is the FIRST step when defining new human resource requirements?
A. Benchmark to an industry peer
B. Request additional funding for recruiting and training
C. Determine the security technology requirements for the initiatives

D. Analyze the skills necessary to support the new initiatives.
Answer: (SHOW ANSWER)

NEW QUESTION: 43
A newly hired information security manager discovers that the cleanup of accounts for terminated employees happens only once a year. Which of the following should be the information security manager's FIRST course of action?
A. Update the security policy
B. Design and document a new process
C. Report the issue to senior management
D. Perform a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Information security governance is PRIMARILY driven by which of the following?
A. Technology constraints
B. Regulatory requirements
C. Business strategy
D. Litigation potential
Answer: (SHOW ANSWER)

NEW QUESTION: 45
The PRIMARY purpose of a security information and event management (SIEM) system is to:
A. provide status of incidents
B. track ongoing incidents
C. identify potential incidents.
D. resolve incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which of the following is the MOST useful metric for determining how well firewall logs are being monitored?
A. The number of investigated alerts
B. The number of dropped malformed packets
C. The number of log entries reviewed
D. The number of port scanning attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 47
When determining an acceptable risk level, which of the following is the MOST important consideration?
A. Vulnerability scores
B. System criticality
C. Threat profile
D. Risk matrices
Answer: (SHOW ANSWER)

NEW QUESTION: 48
An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:
A. identify security program gaps or systemic weaknesses that need correction.
B. prepare properly vetted notifications regarding the incidents to external parties
C. identify who should be held accountable for the security incidents.
D. document and report the root cause of the incidents for senior management
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?
A. The ability to meet deliverables
B. The cost of the services
C. The vendor's reputation m the industry
D. The business need for the function
Answer: (SHOW ANSWER)

NEW QUESTION: 50
A new program has been implemented to standardize security configurations across a multinational organization Following implementation, the configuration standards should:

A. be updated to address emerging threats and vulnerabilities.
B. remain unchanged to avoid variations across the organization
C. be changed for different subsets of the systems to minimize impact,

D. not deviate from industry best practice baselines.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
The GREATEST benefit of choosing a private cloud over a public cloud would be:
A. server protection.
B. containment of customer data,
C. collection of data forensic
D. online service availability.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following is the MOST important factor to ensure information security is meeting the organization's objectives?
A. Implementation of a control self-assessment (CSA) process
B. Implementation of a security awareness program
C. Establishment of acceptable risk thresholds
D. Internal audit's involvement in the security process
Answer: (SHOW ANSWER)

NEW QUESTION: 53
The use of a business case to obtain funding for an information security investment is MOST effective when the business case:
A. articulates management s intent and information security directives in clear language.
B. translates information security policies and standards into business requirements.
C. realigns information security objectives to organizational strategy,
D. relates the investment to the organization's strategic plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which of the following will BEST help to ensure security is addressed when developing a custom application?
A. Integrating security requirements into the development process
B. Conducting security training for the development staff
C. Requiring a security assessment before implementation
D. Integrating a security audit throughout the development process
Answer: (SHOW ANSWER)

NEW QUESTION: 55

An information security manager is evaluating the key risk indicators (KRIs) for an organization s information security program. Which of the following would be the information security manager s GREATEST concern?
A. Lack of formal KRI approval from IT management
B. Multiple KRIs for a single control process
C. Undefined thresholds to trigger alerts
D. Use of qualitative measures
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which of the following is MOST likely to increase end user security awareness in an organization?
A. A dedicated channel for reporting suspicious emails
B. Simulated phishing attacks
C. Red team penetration testing
D. Security objectives included in job descriptions
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which of the following should be the PRIMARY expectation of management when an organization introduces an information security governance framework?
A. Consistent execution of information security strategy
B. Improved accountability to shareholders
C. Increased influence of security management
D. Optimized information security resources
Answer: (SHOW ANSWER)

NEW QUESTION: 58
An information security manager is asked to provide a short presentation on the organization's current IT risk posture to the board of directors. Which of the following would be MOST effective To include in this presentation?
A. Risk register
B. Gap analysis results
C. Threat assessment results
D. Risk heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 59
When establishing the trigger levels for an organization's key risk indicators (KRIs), the thresholds should be based PRIMARILY on the organization's:
A. risk appetite.

B. risk register.
C. risk response capability.
D. current threat level.
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Which of the following is the BEST reason for delaying the application of a critical security patch?
A. Resource limitations
B. Lack of vulnerability management
C. Technology interdependences
D. Conflicts with software development life cycle
Answer: (SHOW ANSWER)

NEW QUESTION: 61
In a risk assessment after the identification of threats to organizational assets, the information security manager would:
A. determine threats to be reported to upper management.
B. request funding for the security program.
C. evaluate the controls currently in place.
D. implement controls to achieve target risk levels.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?
A. Analyze vulnerabilities
B. Define the recovery point objective (RPO).
C. Determine recovery priorities.
D. Confirm control effectiveness
Answer: (SHOW ANSWER)

NEW QUESTION: 63
The PRIMARY reason for classifying assets is to:

A. inform senior management of the organization's risk posture.
B. establish clear lines of authority and ownership for the asset
C. balance asset value and protection measures.
D. identify low-value assets with insufficient controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following is the BEST way for an information security manager to justify continued investment in the information security program when the organization is facing significant budget cuts?
A. Demonstrate an increase in ransomware attacks targeting peer organizations.
B. Demonstrate the readiness of business continuity plans.
C. Demonstrate that the program enables business activities.
D. Demonstrate that implemented program controls are effective.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following is MOST helpful in protecting against hacking attempts on the production network?
A. Network penetration testing
B. Intrusion prevention systems
C. Decentralized honeypot networks
D. Security information and event management (SIEM) tools
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following is MOST critical for an effective information security governance framework?
A. The CIO is accountable for the information security program.
B. Information security policies are reviewed on a regular basis.
C. Board members are committed to the information security program
D. The information security program is continually monitored.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers and maintaining all core business functions in-house. The information security manager has determined a defense in depth strategy should be used. Which of the following BEST describes this strategy?
A. Deployment of nested firewalls within the infrastructure
B. Separate security controls for applications, platforms programs and endpoints

C. Multi-factor login requirements for cloud service applications timeouts, and complex passwords
D. Strict enforcement of role-based access control (RBAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 68
A hacking group has posted an organization's employee data on social media. What should the information security manager do FIRST?
A. Review system audit logs.
B. Inform the impacted employees.
C. Notify law enforcement.
D. Initiate the incident response process.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Which of the following is the MOST effective method for categorizing system and data criticality during the risk assessment process?
A. Interview members of the board.
B. Interview data custodians.
C. Interview the asset owners.
D. Interview senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 70
What should be an information security manager's FIRST course of action upon learning of a security threat that has occurred in the industry for the first time?

A. Perform a control gap analysis of the organization's environment
B. Examine responses of victims that have been exposed to similar threats.
C. Revise the organization's incident response plan.
D. Update the relevant information security policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
An information security manager has been alerted to a possible incident involving a breach at one of the organization's vendors. Which of the following should be done FIRST?
A. Perform incident eradication.
B. Perform incident recovery.
C. Discontinue the relationship with the vendor.
D. Engage the incident response team.
Answer: (SHOW ANSWER)

NEW QUESTION: 72

Which of the following would provide nonrepudiation of electronic transactions?
A. Third-party certificates
B. Two-factor authentication
C. Periodic reaccreditations
D. Receipt acknowledgment
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following is MOST important for the effectiveness of an incident response function?
A. Automated modem tracking and reporting tools
B. Establishing prior contacts with law enforcement
C. Enterprise security management system and forensic tools
D. Training of all users on when and how to report
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?
A. Enforce passwords and data encryption on the devices.
B. Conduct security awareness training.
C. Review and update existing security policies.
D. Require remote wipe capabilities for devices.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following would BEST fulfill a board of directors' request for a concise
A. Balanced scorecard
B. Risk heat map
C. Business impact analysis
D. Risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following is the BEST way to increase the visibility of information security within an organization's culture?
A. Establishing security policies based on industry standards
B. Implementing user awareness campaigns for the entire company
C. Requiring cross-functional information security training
D. Publishing an acceptable use policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
Which of the following is BEST determined by using technical metrics?
A. Whether security resources are adequately allocated
B. How well security risk is being managed
C. Whether controls are operating effectively.
D. How well the security strategy is aligned with organizational objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 78
An organization involved in e-commerce activities operating from its home country opened a new office in another country wit! stringent security laws. In this scenario, the overall security strategy should be based on:
A. risk assessment results.
B. the security organization structure
C. international security standards.
D. the most stringent requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
An organization has implemented an enhanced password policy for business applications which requires significantly more business resource to support clients. The BEST approach to obtain the support of business management would be to:
A. Present industry benchmarking results to business units
B. Present an analysis of the cost and benefit of the changes
C. Discuss the risk and impact of security incidents if not implemented
D. Elaborate on the positive impact to information security
Answer: (SHOW ANSWER)

NEW QUESTION: 80
In addition to cost what is the BEST criteria for selecting countermeasures following a risk assessment?
A. Effort of implementation
B. Effectiveness of each option

C. Skill requirements for implementation
D. Maintenance requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following is MOST important to consider when developing a disaster recovery plan?
A. Business continuity plan (BCP)
B. Feasibility assessment
C. Cost-benefit analysis
D. Business impact analysis (BIA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
The BEST way to identify the criticality of systems to the business is through:
A. a vulnerability assessment.
B. an impact assessment.
C. a threat assessment.
D. an asset classification.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following is MOST effective against system intrusions?
A. Two-factor authentication
B. Penetration testing
C. Layered protection
D. Continuous monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following is the GREATEST risk associated with the head of information security reporting to the chief information officer (CIO)?
A. Insufficient authority to perform duties effectively
B. Duplicate roles and responsibilities
C. Inadequate IT security controls to protect FT assets
D. Conflict of interest while running IT operations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
To implement a security framework, an information security manager must FIRST develop:
A. a security policy
B. security standards.

C. security guidelines
D. security procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 86
An organization has concerns regarding a potential advanced persistent threat (APT). To ensure that the risk associated with this threat is appropriately managed, what should be the organization 5 FIRST action?
A. Implement additional controls.
B. Initiate incident response processes.
C. Report to senior management.
D. Conduct an impact analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following is the MOST effective method for assessing the effectiveness of a security awareness program?
A. Social engineering test
B. Vulnerability scan
C. Tabletop test
D. Post-incident review
Answer: (SHOW ANSWER)

NEW QUESTION: 88
The MAIN reason for an information security manager to monitor industry level changes in the business and FT is to:
A. update information security policies in accordance with the changes
B. change business objectives based on potential impact
C. identify changes in the risk environment
D. evaluate the effect of the changes on the levels of residual risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Which of the following is the FIRST step to promoting acceptable behavior with regard to information security throughout an organization?
A. Conduct targeted acceptable use training for management and staff.
B. Automate controls that enforce acceptable use.
C. Require signed acknowledgment of acceptable use policies.
D. Incorporate information security standards into performance evaluations.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Which of the following BEST supports the alignment of information security with business functions?
A. Creation of a security steering committee
B. A focus on technology security risk within business processes
C. Business management participation in security penetration tests
D. IT management support of security assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 91
After adopting an information security framework, an information security manager is working with senior management to change the organization-wide perception that information security is solely the responsibility of the information security department. To achieve this objective, what should be the information security manager's FIRST initiative?
A. Document and publish the responsibilities of the information security department
B. Develop an operational plan providing best practices for information security projects.
C. Develop an information security awareness campaign with senior managements support.
D. Implement a formal process to conduct periodic compliance reviews.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Which of the following is the BEST approach for an information security manager to effectively manage third-party risk?
A. Ensure vendor governance controls are in place.
B. Ensure senior management has approved the vendor relationship.
C. Ensure controls are implemented to address changes in risk.
D. Ensure risk management efforts are commensurate with risk exposure.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
During the restoration of several servers, a critical process that services external customers was restored late due to a failure, resulting in lost revenue. Which of the following would have BEST helped to prevent this occurrence?

A. Validation of senior management's risk tolerance
B. Improvements to incident identification methods
C. Updates to the business impact analysis (BIA)
D. More effective disaster recovery plan (DRP) testing
Answer: (SHOW ANSWER)

NEW QUESTION: 94
What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?
A. Communicate incident response procedures to staff.
B. Test incident response procedures regularly.
C. Establish and measure key performance indicators (KPIs)
D. Obtain senior management commitment
Answer: (SHOW ANSWER)

NEW QUESTION: 95
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:
A. map the business process to supporting IT and other corporate resources.
B. identify critical processes and the degree of reliance on support services.
C. obtain the support of executive management.
D. document the disaster recovery process.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
After assessing risk, the decision to treat the risk should be based PRIMARILY on:
A. whether the level of risk exceeds inherent risk.
B. the criticality of the risk.
C. availability of financial resources.
D. whether the level of risk exceeds risk appetite.
Answer: (SHOW ANSWER)

NEW QUESTION: 97
An organization has recently experienced unauthorized device access to its network. To proactively manage the problem and mitigate this risk, the BEST preventive control would be to:
A. deploy an automated asset inventory discovery tool to identify devices that access the network
B. keep an inventory of network and hardware addresses of all systems connected to the network
C. install a stateful inspection firewall to prevent unauthorized network traffic
D. implement network-level authentication and login to regulate access of devices to the network
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following is MOST likely to be included in an enterprise information security policy?
A. Consequences of noncompliance
B. Password composition requirements
C. Security monitoring strategy
D. Audit trail review requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Annual risk assessments
B. Business impact analysts
C. Security baselining
D. Continuous monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Which of the following statements indicates that a previously failing security program is becoming successful?

A. The number of vulnerability false positives is decreasing.
B. The number of threats has been reduced.
C. More employees and stakeholders are attending security awareness programs.
D. Management's attention and budget are now focused on risk reduction.
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Which of the following will BEST ensure that risk is evaluated on system level changes?
A. Security should be integrated in the change control process.
B. Implement a centralized change management system.
C. Senior management must sign-off on changes.
D. System development staff receives regular security training.
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Authorization can BEST be accomplished by establishing:
A. whether users are who they say they are
B. who users can do when they are granted system access.
C. how users identify themselves to information systems.
D. the ownership of the data
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Which is MOST important to enable a timely response to a security breach?
A. Security event logging
B. Forensic analysis
C. Knowledge sharing and collaboration
D. Roles and responsibilities
Answer: (SHOW ANSWER)

NEW QUESTION: 104
A new organization has been hit with a ransomware attack that is critically impacting its business operations.
The organization does not yet have a proper incident response plan, but it does have a backup procedure for restoration of data. Which of the following should be the FIRST course of action?
A. Recommend that management pay the ransom.
B. Establish an incident response plan.
C. Isolate the affected system.
D. Contact the legal department.
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Information security governance is PRIMARILY a:
A. process issue.
B. people issue.
C. business issue.
D. regulatory issue.
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which of the following is BEST performed by the security department?
A. Logging unauthorized access to the operating system
B. Managing user profiles for accessing the operating system
C. Provisioning users to access the operating system
D. Approving standards for accessing the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Which of the following is the MOST useful input for an information security manager when refreshing the organizations security strategy?
A. Results of a security pokey review
B. Results of a security risk assessment
C. Results of a red team exercise
D. Results of a vulnerability scan
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which of the following would contribute MOST to employees' understanding of data handling responsibilities?
A. Labeling documents according to appropriate security classification
B. Implementing a tailored security awareness training program
C. Requiring staff acknowledgement of security policies
D. Demonstrating support by senior management of the security program
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which of the following would BEST detect malicious damage arising from an internal threat?
A. Fraud awareness training
B. Encryption
C. Access control list
D. Job rotation
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following is the MOST effective method to help ensure information security incidents are reported?

A. Integrating information security language in corporate compliance rules
B. Integrating information security language in conditions of employment
C. Providing information security awareness training to employees
D. Implementing an incident management system
Answer: (SHOW ANSWER)

NEW QUESTION: 111

To ensure adequate disaster-preparedness among IT infrastructure personnel, it is MOST important to:
A. periodically rotate recovery-test participants.
B. include end-user personnel in each recovery test.
C. have the most experienced personnel participate in recovery tests.
D. assign personnel-specific duties in the recovery plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
The MOST important reason to use a centralized mechanism to identify information security incidents is to:
A. detect potential fraud.
B. comply with corporate policies
C. detect threats across environments
D. prevent unauthorized changes to networks
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Risk reporting requirements should be PRIMARILY based on:
A. policies approved by information security.
B. criteria approved by management,
C. events defined by information security.
D. the criticality of assets.
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which of the following would provide the BEST justification for a new information security investment?
A. Defined key performance indicators (KPIs)
B. Results of a comprehensive threat analysis
C. Senior management involvement in project prioritization
D. Projected reduction in risk
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following should be the PRIMARY input when defining the desired state of security within an organization?
A. External audit results
B. Level of business impact
C. Acceptable risk level
D. Annual loss expectancy

Answer: (SHOW ANSWER)

NEW QUESTION: 116
During the establishment of a service level agreement (SLA) with a cloud service provider, it is MOST important for the information security manager to:
A. set up proper communication paths with the provider.
B. ensure security requirements are contractually enforceable.
C. update the security policy to reflect the provider's terms of service.
D. understand the cloud storage architecture in use to determine security risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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. Terminate the agreement with the third-party contractor
C. Include security requirements in outsourcing contracts
D. Limit access to the third-party contractor
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which of the following is the MOST important step in risk ranking?
A. Threat assessment
B. Vulnerability analysis
C. Impact assessment
D. Mitigation cost
Answer: (SHOW ANSWER)

NEW QUESTION: 119
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. Design mitigating controls for the exceptions.
B. Report the noncompliance to the board of directors.
C. Inform respective risk owners of the impact of exceptions.
D. Prioritize the risk and implement treatment options.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which of the following is a PRIMARY responsibility of an information security governance committee'
A. Approving the information security awareness training strategy

B. Analyzing information security policy compliance reviews
C. Approving the purchase of information security technologies
D. Reviewing the information security strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Which of the following should be the PRIMARY consideration when developing a security governance framework for an enterprise?
A. Benchmarking against industry best practice
B. Understanding of the current business strategy
C. Results of a business impact analysis (BIA)
D. Assessment of the current security architecture
Answer: (SHOW ANSWER)

NEW QUESTION: 122
When aligning an organization's information security program with other risk and control activities, it is MOST important to:
A. ensure adequate financial resources are available,.
B. have information security management report to the chief risk officer.
C. integrate security within the system development life cycle.
D. develop an information security governance framework.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following is MOST important to consider when determining asset valuation?
A. Cost of insurance premiums
B. Potential business loss
C. Asset classification level
D. Asset recovery cost
Answer: (SHOW ANSWER)

NEW QUESTION: 124

An organization us& a particular encryption protocol for externally facing web pages and key financial services. A security firm publicizes a critical security flaw in the encryp manager do FIRST?

A. Activate the incident response team.

B. Isolate potentially vulnerable systems.

C. Remediate the vulnerability.

D. Perform a risk assessment.

Answer: (SHOW ANSWER)

NEW QUESTION: 125

When integrating information security requirements into software development, which of the following practices should be FIRST in the development lifecycle?

A. Threat modeling

B. Dynamic code analysis

C. Penetration testing

D. Source code review

Answer: A (LEAVE A REPLY)

NEW QUESTION: 126

Recovery time objectives (RTOs) are an output of which of the following?

A. Disaster recovery plan

B. Service level agreement (SLA)

C. Business impact assessment (BIA)

D. Business continuity plan

Answer: (SHOW ANSWER)

NEW QUESTION: 127

Which of the following is the BEST indication of an effective information security program?

A. Policies are approved by senior management.

B. Key risk indicators (KRIs) are established.

C. Risk is treated to an acceptable level.

D. Policies and standards are developed.

Answer: (SHOW ANSWER)

NEW QUESTION: 128

For proper escalation of events, it is MOST important for the information security manager to ensure:

A. incident severity levels are defined.

B. the incident team is adequately staffed.

C. the incident response plan is approved.

D. incident documentation templates are created.

Answer: (SHOW ANSWER)

NEW QUESTION: 129
Which of the following is the GREATEST security threat when an organization allows remote access through a virtual private network (VPN)?
A. VPN traffic could be sniffed and captured.
B. Client logins are subject to replay attack.
C. Attackers could compromise the VPN gateway.
D. Compromised VPN clients could impact the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?

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

NEW QUESTION: 131
A new mobile application is unable to adhere to the organization's authentication policy. Which of the following would be the information security manager's BEST course of action?
A. Include historical data of reported incidents.
B. Provide the estimated return on investment (ROI).
C. Provide an analysis of current risk exposures.
D. Include industry benchmarking comparisons.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
Who is MOST important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data toss?
A. An independent auditor for identification of control deficiencies
B. A forensics expert for evidence management
C. A penetration tester to validate the attack
D. A damage assessment expert for calculating losses
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Which of the following would BEST enhance firewall security?
A. Implementing change-control practices

B. Placing the firewall on a screened subnet
C. Logging of security events
D. Providing dynamic address assignment
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which of the following BEST enables an effective escalation process within an incident response program?
A. Dedicated funding for incident management
B. Monitored program metrics
C. Defined incident thresholds
D. Adequate incident response staffing
Answer: (SHOW ANSWER)

NEW QUESTION: 135
An organization is developing a disaster recover/ plan for a data center that hosts multiple applications. The application recovery sequence would BEST be determined through an analysis of:
A. Key performance indicators (KPIs)
B. Recovery point objectives (RPOs)
C. Recovery time objectives (RTOs)
D. The data classification scheme.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following BEST contributes to the successful management of security incidents?
A. Current technologies
B. Tested controls
C. Established procedures
D. Established policies
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Following a recent acquisition, an information security manager has been requested to address the outstanding risk reported early in the acquisition process. Which of the following is the manager s BEST course of action?
A. Add the outstanding risk to the acquiring organization's risk registry
B. Perform a vulnerability assessment of the acquired company s infrastructure.
C. Re-evaluate the risk treatment plan for the outstanding risk.
D. Re-assess the outstanding risk of the acquired company.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
To prevent computers on the corporate network from being used as part of a distributed denial of service (DDoS) attack, the information security manager should use:
A. outgoing traffic filtering.
B. IT security policy dissemination.
C. incoming traffic filtering.
D. rate limiting.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
For an organization with a large and complex IT infrastructure, which of the following elements of a disaster recovery hot site service will require the closest monitoring?
A. Number of subscribers
B. Employee access
C. Audit tights
D. Systems configurations
Answer: (SHOW ANSWER)

NEW QUESTION: 140
A PRIMARY advantage of involving business management in evaluating and managing information security risks is that they:

A. better understand organizational risks.
B. are more objective than security management,
C. better understand the security architecture.
D. can balance technical and business risks.
Answer: (SHOW ANSWER)

NEW QUESTION: 141
After undertaking a security assessment of a production system, the information security manager is MOST likely to:
A. inform the system owner of any residual risks and propose measures to reduce them.

B. inform the IT manager of the residual risks and propose measures to reduce them.
C. inform the development team of any residual risks and together formulate risk reduction measures.
D. establish an overall security program that minimizes the residual risks of that production system
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Which of the following is the MOST effective data loss control when connecting a personally owned mobile device to the corporate email system?
A. Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
B. Users must agree to allow the mobile device to be wiped if it is lost
C. Email must be stored in an encrypted format on the mobile device
D. A senior manager must approve each new connection
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Labeling information according to its security classification:
A. enhances the likelihood of people handling information securely,
B. reduces the need to identify baseline controls for each classification.
C. affects the consequences if information is handled insecurely,
D. induces the number and type of counter measures required
Answer: (SHOW ANSWER)

NEW QUESTION: 144
An information security manager is asked to provide evidence that the organization is fulfilling its legal obligation to protect personal identifiable information (PII). Which of the f<
A. Risk assessments of privacy-related applications
B. Privacy awareness training
C. Metrics related to program effectiveness
D. Written policies and standards
Answer: (SHOW ANSWER)

NEW QUESTION: 145
An organization planning to contract with a cloud service provider is concerned about the risk of account hijacking at login. What is MOST important for the organization in its security requirements to address this concern?
A. Create unique login credentials for each user.
B. Utilize multi-factor authentication
C. Rotate account passwords regularly.
D. Utilize encryption for account logins.

Answer: (SHOW ANSWER)

NEW QUESTION: 146
Before final acceptance of residual risk, what is the BEST way for an information security manager to address risk factors determined to be lower than acceptable risk levels?
A. Ask senior management to lower the acceptable risk levels.
B. Evaluate whether an excessive level of control is being applied.
C. Ask senior management to increase the acceptable risk levels
D. Implement more stringent countermeasures.
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which of the following processes is the FIRST step in establishing an information security policy?
A. Information security audit
B. Business risk assessment
C. Security controls evaluation
D. Review of current global standards
Answer: (SHOW ANSWER)

NEW QUESTION: 148
Which of the following is the MOST important function of information security?
A. Preventing security incidents
B. Identifying system vulnerabilities
C. Reducing the financial impact of security breaches
D. Managing risk to the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 149
Which of the following would be MOST helpful to an information security manager tasked with enforcing enhanced password standards?
A. Reeducating end users on creating strong, complex passwords
B. Implementing a centralized identity management system
C. Implementing technical password controls to include strong complexity
D. Conducting password strength testing
Answer: (SHOW ANSWER)

NEW QUESTION: 150
When selecting risk response options to manage risk, an information security manager's MAIN focus should be on reducing:

A. financial loss by transferring risk.
B. exposure to meet risk tolerance levels.

C. the likelihood of threat.
D. the number of security vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 151
The PRIMARY purpose of asset valuation for the management of information security is to:
A. provide a basis for asset classification.
B. determine the value of each asset
C. eliminate the least significant assets.
D. prioritize risk management activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 152
In information security governance, the PRIMARY role of the board of directors is to ensure:
A. compliance with regulations and best practices
B. alignment with the strategic goals of the organization
C. communication of security posture to stakeholders.
D. approval of relevant policies and standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 153
When developing an information security governance framework, which of the following should be the FIRST activity?
A. Develop response measures to detect and ensure the closure of security breaches.
B. Develop policies and procedures to support the framework.
C. Align the information security program with the organization's other risk and control activities.
D. Integrate security within the system's devetoojtam life cycle process.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
When preventative controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager to perform?

A. Manage the impact.
B. Evaluate potential threats.
C. Identify unacceptable risk levels.
D. Assess vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which of the following would be MOST important to consider when implementing security settings for a new system'
A. Results from internal and external audits
B. Industry best practices applicable to the business
C. Business objectives and related IT risk
D. Government regulations and related penalties
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Which of the following is the PRIMARY benefit of using a tabletop method to conduct an incident response exercise?
A. The impact of IT systems on business operations is quantified.
B. Visibility into personnel effectiveness is increased.
C. Potential impact to business operations is minimized.
D. The readiness of applications for testing is ensured.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
An organization is considering a self-service solution for the deployment of virtualized development servers.
Which of the following should be information security manager's PRIMARY concern?
A. Segregation of servers from the production environment
B. Ability to remain current with patches
C. Ability to maintain server security baseline
D. Generation of excessive security event logs
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Which of the following enables compliance with a nonrepudiation policy requirement for electronic transactions?
A. One-time passwords
B. Digital certificates
C. Encrypted passwords
D. Digital signatures

Answer: (SHOW ANSWER)

NEW QUESTION: 159
Which of the following would be MOST helpful to reduce the amount of time needed by an incident response team to determine appropriate actions?
A. Validating the incident response plan against industry best practices
B. Rehearsing incident response procedures rote, and responsibilities
C. Providing annual awareness training regarding incident response for team members
D. Defining modern seventy levels during a business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 160
Which of the following is the KEY outcome of conducting a post-incident review?
A. Chain of custody is maintained.
B. Root cause is validated.
C. Compliance requirements are met.
D. Risk appetite is validated.
Answer: (SHOW ANSWER)

NEW QUESTION: 161
The PRIMARY reason for implementing scenario-based training for incident response is to:
A. verify threats and vulnerabilities faced by the incident response team.
B. assess the timeliness of the incident team response and remediation.
C. help incident response team members understand their assigned roles.
D. ensure staff knows where to report in the event evacuation is required.
Answer: (SHOW ANSWER)

NEW QUESTION: 162
An information security program should be established PRIMARILY on the basis of:
A. data security regulatory requirements.
B. the approved risk management approach.
C. the approved information security strategy.
D. senior management input
Answer: (SHOW ANSWER)

NEW QUESTION: 163
When trying to integrate information security across an organization, the MOST important goal for a governing body should be to ensure:
A. periodic information security audits are conducted.
B. information security is treated as a business critical issue.
C. the resources used for information security projects are kept to a minimum.

D. funding is approved for requested information security projects.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
An employee is found to be using an external cloud storage service to share corporate information with a third-party consultant, which is against company policy. Which of the following should be the information security manager s FIRST course of action?
A. Seek business justification from the employee
B. Block access to the cloud storage service.
C. Determine the classification level of the information
D. Inform higher management of a security breach
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Conducting a cost-benefit analysis for a security investment is important because it
A. quantifies residual risk
B. supports asset classification.
C. quantifies return on security investment
D. supports justification for expenditure.
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Establishing which of the following is the BEST way of ensuring that the emergence of new risk is promptly identified?
A. Regular risk repotting
B. Risk monitoring processes
C. Incident monitoring activities
D. Change control procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 167
The FIRST step in establishing an information security program is to:

A. assess the organization s compliance with regulatory requirements
B. define polices and standards that mitigate the organization's risks.
C. determine the level of risk that is acceptable to some management
D. secure organizational commitment and support
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which of the following is the MOST relevant risk factor to an organization when employees use social media?
A. Social media offers a platform that can host cyber-attacks.
B. Social media increases the velocity of risk and the threat capacity.
C. Social media can be used to gather intelligence for attacks.
D. Social media can be accessed from multiple locations.
Answer: (SHOW ANSWER)

NEW QUESTION: 169
An organization wants to integrate information security into its human resource management processes. Which of the following should be the FWST step?
A. Evaluate the cost of information security integration
B. Benchmark the processes with best practice to identify gaps.
C. Identify information security risk associated with the processes
D. Assess the business objectives of the processes
Answer: (SHOW ANSWER)

NEW QUESTION: 170
An organization is concerned with the risk of information leakage caused by incorrect use of personally owned smart devices by employees. What is the BEST way for the information security manager to mitigate the associated risk?

A. Require employees to sign a nondisclosure agreement
B. Document a bong-your-own-device (BYOD) policy.
C. Implement a mobile device management solution.
D. implement a multi-factor authentication solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
What would be an information security manager's BEST course of action when notified that the implementation of some security controls is being delayed due to budget constraints?
A. Request a budget exception for the security controls
B. Prioritize security controls based on risk.
C. Begin the risk acceptance process
D. Suggest less expensive alternative security controls.

Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which of the following sites is MOST appropriate in the case of a very short recovery time objective (RTO)?
A. Mobile
B. Shared
C. Redundant
D. Warm
Answer: (SHOW ANSWER)

NEW QUESTION: 173
An information security manager is developing a new information security strategy. Which of the following functions would serve as the BEST resource to review the strategy and provide guidance for business alignment?
A. The board of directors
B. The legal department
C. Internal audit
D. The steering committee
Answer: (SHOW ANSWER)

NEW QUESTION: 174
Which of the following is the MOST challenging aspect of securing Internet of Things (IoT) devices?
A. Evaluating the reputations of IoT vendors
B. Managing the diversity of IoT architecture
C. Updating policies to include IoT devices
D. Training staff on IoT architecture
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which of the following would BEST mitigate identified vulnerabilities in a timely manner?
A. Monitoring of key risk indicators (KRIs)
B. Categorization of the vulnerabilities based on system's criticality
C. Continuous vulnerability monitoring tool
D. Action plan with responsibilities and deadlines
Answer: D (LEAVE A REPLY)

NEW QUESTION: 176

A financial institution's privacy department has requested the implementation of multi-factor authentication to comply with regulations for providing services over the Internet. Which of the following authentication schemes would BEST meet this compliance requirement?

A. Username and password

B. Passphrase and token key

C. Four-digit PIN and secret question

D. Thumbprint and facial recognition

Answer: (SHOW ANSWER)

NEW QUESTION: 177

Which of the following is MOST important for an information security manager to communicate to senior management regarding the security program?

A. Potential risks and exposures

B. Security architecture changes

C. User roles and responsibilities

D. Impact analysis results

Answer: (SHOW ANSWER)

NEW QUESTION: 178

An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST"

A. Security operations team

B. Data owners

C. Application owners

D. Communications department

Answer: (SHOW ANSWER)

NEW QUESTION: 179

Which of the following should be the MOST important criteria when defining data retention policies?

A. Capacity requirements

B. Industry best practices

C. Regulatory requirements

D. Audit findings

Answer: (SHOW ANSWER)

NEW QUESTION: 180

Knowing which of the following is MOST important when the information security manager is seeking senior management commitment?

A. Implementation tasks

B. Security costs

C. Security technology requirements
D. Technical vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 181
An organization has decided to implement a security information and event management (SIEM) system. It is MOST important for the organization to consider:
A. data ownership.
B. industry best practices.
C. threat assessments.
D. log sources.
Answer: (SHOW ANSWER)

NEW QUESTION: 182
When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?
A. Firewall logs
B. The security awareness programs
C. Post-incident analysis results
D. The risk management processes
Answer: (SHOW ANSWER)

NEW QUESTION: 183
When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:
A. review the residual risk level
B. implement controls to mitigate the risk.
C. monitor for business changes.
D. report compliance to management
Answer: (SHOW ANSWER)

NEW QUESTION: 184

The effectiveness of security awareness programs in fostering positive security cultures is MOST dependent upon employee:
A. ability to carry out security-related procedures.
B. ownership of security responsibilities.
C. understanding of the penalties for noncompliance.
D. awareness of regulatory requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 185
What should the information security manager do FIRST when end users express that new security controls are too restrictive?
A. Conduct a business impact analysis (BIA).
B. Perform a risk assessment on modifying the control environment.
C. Perform a cost-benefit analysis on modifying the control environment
D. Obtain process owner buy-in to remove the controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 186
Which of the ager to regularly report to senior management?
A. Audit reports
B. Impact of untreated risks
C. Results of penetration tests
D. Threat analysis reports
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which of the following is the MOST important action when using a web application that has recognized vulnerabilities?
A. Monitor application level logs.
B. Install anti-spyware software.
C. Deploy host-based intrusion detection.
D. Deploy an application firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 188
An organization s senior management wants to allow employees to access an internal application using their personal mobile devices. Which of the following should be the information security managers FIRST course of action?
A. Assess the security risk
B. Develop a personal device policy
C. Conduct security testing

D. Require device encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 189
An organization is considering moving one its critical business application to a cloud hosting service. The cloud provider may not provider the same level of security for its application as the organization. Which of the following will provide the BEST information to help maintain the security posture?
A. Risk assessment
B. Risk governance framework
C. Cloud security strategy
D. Vulnerability assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following is the MOST important consideration when determining the approach for gaining organization-wide acceptance of an information security plan?

A. Organizational information security awareness
B. Information security roles and responsibilities
C. Mature security policy
D. Organizational culture
Answer: (SHOW ANSWER)

NEW QUESTION: 191
Which of the following defines the triggers within a business continuity plan (BCP)?
A. Disaster recovery plan (DRP)
B. Needs of the organization
C. Information security policy
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 192
Several significant risks have been identified after a centralized risk register was compiled and prioritized. The information security manager s MOST important action is to:
A. provide senior management with risk treatment options.
B. ensure that employees are aware of the risk.
C. consult external third parties on how to treat the risk.
D. design and implement controls to reduce the risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 193

Which of the following BEST measures the effectiveness of an organization's information security strategy?
A. Comparison of current security budget to previous year's budget
B. Comparison of mitigated risk to accepted risk
C. Comparison of residual risk to risk appetite
D. Comparison of threats to vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 194
A review of a number of recent XT system rollouts identified a failure to incorporate security within planning, development and implementation. Which of the following is the MOST effective way to prevent a recurrence for future systems?
A. Implement security assessments throughout the systems development life cycle.
B. Train and test system developers m secure coding practices.
C. Require penetration tests before production implementation.
D. Conduct regular security audits during system implementation stages.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
An outsourced vendor handles an organization's business-critical data. Which of the following is the MOST effective way for the client organization to obtain assurance of the vendor's security practices?
A. Requiring business continuity plans (BCPs) from the vendor
B. Reviewing the vendor's security audit reports
C. Verifying security certifications held by the vendor
D. Requiring periodic independent third-party reviews
Answer: B (LEAVE A REPLY)

NEW QUESTION: 196
Which of the following is MOST important for an information security manager to include in a report to senior management following a post-incident review?
A. Lessons learned
B. The incident response plan
C. Detailed metrics
D. Snapshot of system logs
Answer: (SHOW ANSWER)

NEW QUESTION: 197
What should the information security manager recommend to support the development of a new web application that will allow retail customers to view inventory and order products?
A. Access through a virtual private network (VPN)
B. Request customers adhere to baseline security standards
C. Implementation of secure transmission protocols
D. Building an access control matrix
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Which of the following is the MOST effective way to mitigate the risk of confidential data leakage to unauthorized stakeholders?
A. Require the use of login credentials and passwords.
B. Create a data classification policy.
C. Implement role-based access controls.
D. Conduct information security awareness training.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 199
Which of the following is the MOST important prerequisite to performing an information security risk assessment?
A. Classifying assets
B. Assessing threats and vulnerabilities
C. Determining risk tolerance
D. Reviewing the business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 200
Which of the following should be the FIRST course of action when it becomes apparent that the recovery time objective (RTO) will not be met during incident response

A. Notify the risk management team.
D Modify the RTO as needed
B. Escalate the emergency status rating.
C. Request additional financial recovery resources.
Answer: (SHOW ANSWER)

NEW QUESTION: 201
Which of the following should be done FIRST when selecting performance metrics to report on the vendor risk management process?
A. Identify the intended audience.
B. Select the data source
C. Review the confidentiality requirements.
D. Identify the data owner.
Answer: (SHOW ANSWER)

NEW QUESTION: 202
An information security manager has identified multiple areas of compliance risk that could subject the organization to significant penalties regarding the handling of personal data. Which of the following is the manager s BEST course of action?
A. Prioritize the risk and present it to senior management.
B. Seek human resources advice to make appropriate changes to the information security policy.
C. Implement information masking controls to hide personal data
D. Immediately update the information security policy to address protection of personal data
Answer: (SHOW ANSWER)

NEW QUESTION: 203
When building a corporate-wide business continuity plan {BCP), it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the BEST method to determine the priority of system recovery in the event of a disaster?
A. Evaluating the cost associated with each system's outage
B. Comparing the recovery point objectives (RPOs)
C. Reviewing each system's key performance indicators (KPIs)
D. Reviewing the business plans of each department
Answer: (SHOW ANSWER)

NEW QUESTION: 204
The BEST way to determine the current state of information security with regard to defined security objectives is by performing a:
A. gap analysis.
B. risk assessment.
C. business impact analysis (BIA).
D. cost-benefit analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 205
The selection of security controls is PRIMARILY linked to:

A. regulatory requirements
B. business impact assessment
C. risk appetite of the organization.
D. best practices of similar organizations.
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which of the following should be the MOST important consideration when implementing an information security framework?
A. Risk appetite
B. Audit findings
C. Compliance requirements
D. Technical capabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 207
An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification foi granting an exception to the policy?
A. Users accept the risk of noncompliance.
B. USB storage devices are enabled based on user roles
C. Access is restricted to read-only.
D. The benefit is greater than the potential risk
Answer: (SHOW ANSWER)

NEW QUESTION: 208
A multinational organization has developed a bring your own device (BYOD) policy that requires the installation of mobile device management (MDM) software on personally owned devices. Which of the following poses the GREATEST challenge for implementing the policy?
A. Differences in corporate cultures
B. Varying employee data privacy rights
C. Differences in mobile OS platforms
D. Translation and communication of policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 209
Which of the following is the BEST approach to identify noncompliance issues with legal, regulatory, and contractual requirements?
A. Risk assessment
B. Vulnerability assessment
C. Business impact analysis (B1A)

D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 210
Which of the following would be MOST useful in a report to senior management for evaluating changes in the organization's information security risk position?

A. Trend analysis
B. Management action plan
C. Industry benchmarks
D. Risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 211
An organization was forced to pay a ransom to regain access to a critical database that had been encrypted in a ransomware attack. What would have BEST prevented The need to make this ransom payment?
A. Training employees on ransomware
B. Ensuring all changes are approved
C. Storing backups on a segregated network.
D. Verifying the firewall is configured properly
Answer: (SHOW ANSWER)

NEW QUESTION: 212
Which of the following would present the GREATEST need to revise information security poll'
A. Implementation of a new firewall
B. An increase in reported incidents
C. A merger with a competing company
D. Changes in standards and procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 213

Which of the following is MOST critical to review when preparing to outsource a data repository to a cloud-based solution?
A. Disaster recovery plan
B. Vendor's information security policy
C. Identity and access management
D. A risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 214
What should an information security team do FIRST when notified by the help desk that an employee's computer has been infected with ma I ware?
A. Use anti-malware software to clean the infected computer.
B. Take a forensic copy of the hard drive.
C. Isolate the computer from the network.
D. Restore the files from a secure backup.
Answer: (SHOW ANSWER)

NEW QUESTION: 215
After a security incident has been contained, which of the following should be done FIRST?
A. Conduct forensic analysis.
B. Restore the affected system from backup.
C. Perform a complete wipe of the affected system.
D. Notify local authorities.
Answer: (SHOW ANSWER)

NEW QUESTION: 216
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. deliver security awareness training.
B. inform senior management of changes in risk metrics.
C. perform an assessment to measure the current state
D. ensure baseline back-ups are performed.
Answer: (SHOW ANSWER)

NEW QUESTION: 217
An organization's IT department is undertaking a large virtualization project to reduce its physical server footprint. Which of the following should be the HIGHEST priority of the information security manager?
A. Selecting the virtualization software
B. Determining how incidents will be managed
C. Ensuring the project has appropriate security funding

D. Being involved at the design stage of the project
Answer: (SHOW ANSWER)

NEW QUESTION: 218
Which of the following would BEST enable an organization to effectively monitor the implementation of standardized configurations?
A. Develop policies requiring use of the established benchmarks.
B. Implement a separate change tracking system to record changes to configurations.
C. Perform periodic audits to detect non-com pliant configurations.
D. Implement automated scanning against the established benchmarks.
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Which of the following is the PRIMARY driver of information security compliance?
A. Regulatory requirements
B. Industry standards
C. Risk appetite
D. Threat environment
Answer: (SHOW ANSWER)

NEW QUESTION: 220
Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?

A. Existence of an industry-accepted framework
B. Up-to-date policy and procedures documentation
C. A report on the maturity of controls
D. Results of an independent assessment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 221
Which of the following is the MOST important requirement for the successful implementation of security governance?
A. Mapping to organizational
B. Aligning to an international security framework
C. Performance an enterprise-wide risk assessment
D. Implementing a security balanced scorecard
Answer: (SHOW ANSWER)

NEW QUESTION: 222

An organization is planning to open a new office in another country. Sensitive data will be routinely sent between the two offices. What should be the information security manager s FIRST course of action?
A. Update privacy policies to include the other country's laws and regulations.
B. Apply the current corporate security policies to the new office.
C. Encrypt the data for transfer to the head office based on security manager approval
D. Identify applicable regulatory requirements to establish security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 223
Which of the following is MOST critical for the successful implementation of an information security strategy?
A. Compliance with regulations
B. Established information security policies
C. Ongoing commitment from senior management
D. Sizeable funding for the information security program
Answer: (SHOW ANSWER)

NEW QUESTION: 224
What should be the PRIMARY basis for establishing a recovery time objective (RTO) for a critical business application?
A. Legal and regulatory requirements
B. Risk assessment results
C. Business impact analysis (BIA) results
D. Related business benchmarks
Answer: (SHOW ANSWER)

NEW QUESTION: 225
Which of the following is an information security manager's BEST course of action to address a significant materialized risk that was not prevented by organizational controls?
A. Update the business impact analysis (BIA)
B. Invoke the incident response plan.
C. Update the risk register.
D. Perform root cause analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Which of the following is the MOST critical security risk to consider for a start-up company in an emerging field?
A. A lack of security policies and procedures
B. Disclosure of financial statements

C. Loss of Intellectual property
D. New entries into the emerging marketplace
Answer: (SHOW ANSWER)

NEW QUESTION: 227
Which of the following metrics is MOST useful to demonstrate the effectiveness of an incident response plan?
A. Average time to resolve an incident
B. Total number of reported incidents
C. Total number of incident responses
D. Average time to respond to an incident
Answer: (SHOW ANSWER)

NEW QUESTION: 228
An information security manager has been made aware that some employees are discussing confidential corporate business on social media sites. Which of the following is the BEST response to this situation?
A. Communicate social media usage requirements and monitor compliance.
B. Scan social media sites for company-related information.
C. Block workplace access to social media sites and monitor employee usage.
D. Train employees how to set up privacy rules on social media sites.
Answer: (SHOW ANSWER)

NEW QUESTION: 229
Which of the following is MOST critical for prioritizing actions in a business continuity plan (BCP)?
A. Business process mapping
B. Risk assessment
C. Business impact analysis (BIA)
D. Asset classification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 230

The PRIMARY disadvantage of using a cold-site recovery facility is that it is:

A. unavailable for testing during normal business hours.

B. only available if not being used by the primary tenant,

C. not possible to reserve test dates m advance

D. not cost-effective for testing critical applications at the site

Answer: (SHOW ANSWER)

NEW QUESTION: 231

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

A. Developing an asset classification model

B. Assigning the asset classification level

C. Securing assets in accordance with their classification

D. Assigning asset ownership

Answer: A (LEAVE A REPLY)

NEW QUESTION: 232

During a review to approve a penetration test plan, which of the following should be an information security managers PRIMARY concern?

A. False positive alarms to operations staff

B. Penetration test team's deviation from scope

C. Impact on production systems

D. Unauthorized access to administrative utilities

Answer: (SHOW ANSWER)

NEW QUESTION: 233

A risk assessment report shows that phishing attacks are an emerging threat for an organization that supports online financial services. Which of the following is the information security manager's BEST course of action?

A. Implement spam protection.

B. Update antivirus software

C. Conduct corporate awareness training.

D. Transfer risk with insurance coverage.

Answer: (SHOW ANSWER)

NEW QUESTION: 234

Which of the following is an example of a vulnerability?

A. Ransomware

B. Unauthorized users

C. Natural disasters

D. Defective software

Answer: (SHOW ANSWER)

NEW QUESTION: 235
Which of the following is the BEST way for an information security manager to identify compliance with information security policies within an organization?
A. Analyze system logs
B. Conduct security awareness testing
C. Conduct per iodic audits.
D. Perform vulnerability assessments
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
An organization implemented a mandatory information security awareness training program a year ago. What is the BEST way to determine its effectiveness?
A. Analyze findings from previous audit reports
B. Analyze responses from an employee survey on training satisfaction
C. Analyze results of a social engineering test
D. Analyze results from training completion reports.
Answer: (SHOW ANSWER)

NEW QUESTION: 237
Threat and vulnerability assessments are important PRIMARILY because they are:
A. the basis for setting control objectives.
B. elements of the organization's security posture.
C. needed to estimate risk.
D. used to establish security investments.
Answer: (SHOW ANSWER)

NEW QUESTION: 238
Which of the following is MOST critical to the successful implementation of information security within an organization?
A. Budget is allocated for information security tools
B. Strong risk management skills exist within the information security group.
C. The information security manager is responsible for setting information security policy.
D. Security is effectively marketed to all managers and employees,
Answer: (SHOW ANSWER)

NEW QUESTION: 239
Which of the following is the PRIMARY objective of the incident management process?
A. To improve security incident response capabilities
B. To reduce the impact of security incidents on the business

C. To reduce the likelihood that security incidents will occur
D. To validate the organization's risk tolerance
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Following a successful and well-publicized hacking incident, an organization alias plans to improve application security. Which of the following is a security project risk?

A. Critical evidence may be lost.
B. The reputation of the organization may be damaged
C. A trapdoor may have been installed m the application.
D. Resources may not be available to support the implementation.
Answer: (SHOW ANSWER)

NEW QUESTION: 241
To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:
A. criteria consistent with classification levels
B. efficient technical processing considerations,
C. overall IT capacity and operational constraints,
D. established guidelines
Answer: (SHOW ANSWER)

NEW QUESTION: 242
Which of the following is the PRIMARY reason to invoke continuity and recovery plans?
A. To coordinate with senior management
B. To protect corporate networks
C. To achieve service delivery objectives
D. To enforce service level agreements (SLAs)
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?

A. Identifying key business risks
B. Identifying critical business processes
C. Identifying the threat environment
D. Identifying risk mitigation options
Answer: (SHOW ANSWER)

NEW QUESTION: 244
When customer data has been compromised, an organization should contact law enforcement authorities:
A. if there is potential impact to the organization.
B. if the attack comes from an international source.
C. in accordance with the corporate communication policy.
D. when directed by the information security manager.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 245
The MOST important reason that security risk assesements should be conducted frequently through an organization is because:
A. Threats to the organization may change
B. Compliance with legal and regulatory should be reassessed.
C. Control effectiveness may weaken.
D. Controls should be regularly tested.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 246
Which of the following is the MOST important outcome of monitoring and reporting on information security processes?
A. Ensuring information security operations meet service level agreements (SLA)
B. Ensiling information security operations follow approved procedures
C. Ensuring information security operations support control objectives
D. Ensuring information security operations are reviewed for effectiveness
Answer: (SHOW ANSWER)

NEW QUESTION: 247
Which of the following would present the GREATEST challenge to integrating information security governance into corporate governance?
A. Information security best practices ant not well understood.
B. key security processes are outsourced.
C. The security organizational structure is loosely defined
D. The information security function is decentralized.
Answer: (SHOW ANSWER)

NEW QUESTION: 248
Which of the following is the PRIMARY benefit of using agentless endpoint security solutions?
A. Decreased network bandwidth usage
B. Increased resiliency
C. Decreased administration
D. More comprehensive information results
Answer: (SHOW ANSWER)

NEW QUESTION: 249
Which of the following is the MOST important consideration when developing an incident management program?
A. Impact assessment
B. IT architecture
C. Risk assessment
D. Escalation procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 250
What should be the information security manager s MOST important consideration when planning a disaster recovery test?

A. Documented escalation processes
B. Stakeholder notification procedures
C. Organization-wide involvement
D. Impact to production systems
Answer: (SHOW ANSWER)

NEW QUESTION: 251
It is MOST important tot an information security manager to ensure that security risk assessments are performed:
A. as part of the security business case
B. In response to the threat landscape,
C. consistently throughout the enterprise.
D. during a root cause analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 252
Which of the following would provide nonrepudiation of electronic transactions?
A. Third-party certificates
B. Periodic reaccredinations
C. Receipt acknowledgment

D. Two-factor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 253
An inexperienced information security manager is relying on its internal audit department to design and implement key security controls. Which of the following is the GREATEST risk?
A. Conflict of interest
B. Violation of the audit charter
C. Inadequate audit skills
D. Inadequate implementation of controls
Answer: (SHOW ANSWER)

NEW QUESTION: 254
It is suspected that key emails have been viewed by unauthorized parties. The email administrator conducted an investigation but it has not returned any information relating to the incident, and leaks are continuing.
Which of the following is the BEST recommended course of action to senior management?
A. Rebuild the email application
B. Commence security training for staff at the organization.
C. Restrict the distribution of confidential emails.
D. Arrange for an independent review.
Answer: (SHOW ANSWER)

NEW QUESTION: 255
Which of the following is the BKT approach for an information security manager when developing new information security policies?
A. Download a policy template
B. Create a stakeholder nap
C. Establish an information security governance committee
D. Reference an industry standard.
Answer: (SHOW ANSWER)

NEW QUESTION: 256
Inadvertent disclosure of internal business information on social media is BEST minimized by which of the following?
A. Limiting access to social media sites
B. Developing social media guidelines
C. Implementing data loss prevention (DLP) solutions
D. Educating users on social media risks
Answer: (SHOW ANSWER)

NEW QUESTION: 257
The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:
A. assign accountability for transactions made with the user's ID.
B. serve as evidence of security awareness training.
C. maintain an accurate record of users access rights
D. maintain compliance with industry best practices.
Answer: (SHOW ANSWER)

NEW QUESTION: 258
Which of the following helps to ensure that the appropriate resources are applied in a timely manner after an incident has occurred?
A. Define incident response teams.
B. Classify the incident
C. Initiate an incident management log
D. Broadcast an emergency message
Answer: (SHOW ANSWER)

NEW QUESTION: 259
Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?
A. Data encryption
B. Data custodian
C. Data monitoring
D. Data ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 260
When developing a disaster recovery plan, which of the following would be MOST helpful in prioritizing the order in which systems should be recovered?

A. Measuring the volume of data in each system
B. Reviewing the business strategy

C. Performing a business impact analysis (BIA)
D. Reviewing the information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 261
Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?
A. The environment is complex.
B. The information regarding monitored activities becomes stale.
C. The activities being monitored deviate from what is considered normal.
D. The pattern of normal behavior changes quickly and dramatically.
Answer: (SHOW ANSWER)

NEW QUESTION: 262
Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?
A. Risk mitigation strategy
B. Security strategy
C. Recovery strategy
D. IT strategy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 263
Which of the following is the BEST option for addressing regulations that will adversely affect the allocation of information security program resources?
A. Delay implementation of compliance activities.
B. Determine compliance levels of peer organizations.
C. Conduct assessments for management decisions.
D. Prioritize compliance efforts based on probability.
Answer: (SHOW ANSWER)

NEW QUESTION: 264
Which of the following should be used to attain sustainable and continuous information security process improvement?
A. Balanced scorecard
B. Plan, Do. Check. Act Process Model
C. Annual audit
D. System development life cycle (SDLC) process
Answer: (SHOW ANSWER)

NEW QUESTION: 265

Which of the following practices BEST supports the achievement of information security program objectives in the IT function?
A. IT management sign-off on information security policies
B. Continuous security auditing of IT service processes
C. Review and approval of IT projects by the information security manager
D. Participation of IT stakeholders in the security program steering committee
Answer: D (LEAVE A REPLY)

NEW QUESTION: 266
Which of the following is MOST important for an information security manager to consider when developing a new information security policy?
A. Organizational goals and objectives
B. Alignment with industry standards
C. Organizational culture and complexity
D. Information security budget allocation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 267
Which of the following measures BEST indicates an improvement in the information security program to stakeholders?
A. A reduction in reported viruses
B. A decrease in click rates during phishing simulations
C. A downward trend in reported security incidents
D. An increase in awareness training quiz pass rates
Answer: (SHOW ANSWER)

NEW QUESTION: 268
What is the MOST important role of an organization's data custodian in support of the information security function?
A. Applying approved security policies
B. Assessing data security risks to the organization
C. Evaluating data security technology vendors
D. Approving access rights to departmental data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 269
An executive's personal mobile device used for business purposes is reported lost. The information security manager should respond based on:
A. incident classification.
B. mobile device configuration.
C. the business impact analysis (BIA).

D. asset management guidelines.
Answer: (SHOW ANSWER)

NEW QUESTION: 270
Which of the following is the MOST effective control to reduce the impact of ransomware attacks?
A. Intrusion detection system (IDS)
B. Backup strategy
C. Antivirus software
D. Security awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 271
An organization has an approved bring your own device (BYOD) program. Which of the following is the MOST effective method to enforce application control on personal devices?
A. Establish a mobile device acceptable use policy
B. Implement a web application firewall.
C. Implement a mobile device management solution.
D. Educate users regarding the use of approved applications.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 272
Which of the following would BEST help to ensure compliance with an organizations information security requirements by an IT service provider?
A. Defining the business recovery plan with the IT service provider
B. Requiring regular reporting from the IT service provider
C. Requiring an external security audit of the IT service provider
D. Defining information security requirements with internal IT
Answer: (SHOW ANSWER)

NEW QUESTION: 273
The integration of information security risk management processes within corporate risk management processes will MOST likely result in:

A. more effective security risk management processes.
B. senior management approval of the information security budgets.
C. improved efficiencies of security operations.
D. information security controls that reduce enterprise risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 274
The BEST defense against phishing attempts within an organization is:
A. strengthening of firewall rules.
B. an intrusion protection system (IPS).
C. an intrusion detection system (IDS).
D. filtering of e-mail.
Answer: (SHOW ANSWER)

NEW QUESTION: 275
When preparing a strategy for protection from SQL injection attacks, it is MOST important for the information security manager to involve:
A. business owners.
B. the security operations center.
C. application developers.
D. senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 276
Which of the following is the MOST important characteristic of an effective security policy?
A. The policy provides broad organizational direction.
B. The policy includes actionable procedures.
C. The policy has been validated by business owners.
D. The policy is aligned to industry best practice.
Answer: (SHOW ANSWER)

NEW QUESTION: 277
An information security manager has researched several options for handling ongoing security concerns and will be presenting these solutions to business managers. Which of the following with BEST enable business managers to make an informed decision?
A. Cost-benefit analysis
B. Risk analysis
C. Business impact analysis (BIA)
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Which of the following is the MOST effective way of ensuring that business units comply with an information security governance framework?
A. Conducting a business impact analysis (BIA)
B. Performing security assessments and gap analyses
C. Conducting information security awareness training
D. Integrating security requirements with processes
Answer: (SHOW ANSWER)

NEW QUESTION: 279
Which of the following techniques is MOST useful when an incident response team needs to respond to external attacks on multiple corporate network devices?
A. Security event correlation analysis
B. Endpoint baseline configuration analysis
C. Vulnerability assessment of network devices
D. Penetration testing of network devices
Answer: (SHOW ANSWER)

NEW QUESTION: 280
A risk management program will be MOST effective when:
A. assessments are repeated periodically
B. business units are involved in risk assessments,
C. risk appetite is sustained for a long period risk
D. risk assessments are conducted by a third party.
Answer: (SHOW ANSWER)

NEW QUESTION: 281
Which of the following BEST demonstrates the maturity of an information security monitoring program?
A. Senior management regularly reviews security standards.
B. The information security program was introduced with a thorough business case.
C. Information security key risk indicators (KRIs) are tied to business operations.
D. Risk scenarios are regularly entered into a risk register.
Answer: (SHOW ANSWER)

NEW QUESTION: 282
Which of the following would be of GREATEST concern to an information security manager when evaluating a cloud service provider (CSP)?
A. There is no right to audit the security of the provider
B. Data retention policies may be violated.
C. Service level agreements (SLAs) art not well defined.

D. Security controls offered by the provider are inadequate
Answer: (SHOW ANSWER)

NEW QUESTION: 283
Which of the following is the PRIMARY reason for performing an analysis of the threat landscape on a regular basis?
A. To determine if existing vulnerabilities present a risk
B. To determine if existing business continuity plans are adequate
C. To determine the basis for proposing an increase in security budgets
D. To determine critical information for executive management
Answer: (SHOW ANSWER)

NEW QUESTION: 284
Which of the following is MOST important to enable after completing action plan?
A. Residual risk
B. Threat profile
C. Inherent risk
D. Vulnerability landscape
Answer: (SHOW ANSWER)

NEW QUESTION: 285
An organization wants to ensure its confidential data is isolated in a multi-tenanted environment at a well-known cloud service provider. Which of the following is the BEST way to ensure the data is adequately protected?
A. Obtain documentation of the encryption management practices.
B. Review the provider's information security policies and procedures.
C. Verify the provider follows a cloud service framework standard.
D. Ensure an audit of the provider is conducted to identify control gaps.
Answer: (SHOW ANSWER)

NEW QUESTION: 286
Which of the following is the BEST way to improve the timely reporting of information security incidents?
A. Incorporate security procedures in help desk processes
B. Integrate an intrusion detection system (IDS) in the DMZ
C. Perform periodic simulations with the incident response team.
D. Regularly reassess and update the incident response plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 287
For an organization with operations in different parts of the world, the BEST approach for ensuring that security policies do not conflict with local laws and regulations is to:
A. refer to an external global standard to avoid any regional conflict
B. adopt uniform policies.
C. make policies at a sufficiently high level, so they are globally applicable.
D. establish a hierarchy of global and local policies.
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**964** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)