ISACA.CISM.v2020-08-26.q208

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	208
Version:	v2020-08-26
# of views:	1836
# of Questions views:	115954
https://www.freecram.net/torrent/ISACA.CISM.v2020-08-26.q208.html	

NEW QUESTION: 1
Which of the following presents the GREATEST concern to the information security manager when using account locking features on an online application? It can increase vulnerability..
A. phishing.
B. brute force attacks.
C. social engineering.
D. denial of service.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
The MAIN reason for an information security manager to monitor industry level changes in the business and FT is to:
A. evaluate the effect of the changes on the levels of residual risk.
B. update information security policies in accordance with the changes
C. change business objectives based on potential impact
D. identify changes in the risk environment
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following is an information security manager's MOST important consideration during the investigative process of analyzing the hard drive of 3 compromises..
A. Determining the classification of stored data
B. Notifying the relevant stakeholders
C. Maintaining chain of custody
D. Identifying the relevant strain of malware
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following is the GREATEST risk to consider when a rival organization purchases a business unit within an organization?
A. Access and permissions to the corporate network from the business unit will remain after the sale.
B. The business unit's confidential information will be transferred to the nval organization during the separation.
C. Senior business management will not understand technical risks.
D. Loss of corporate knowledge.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following is the PRIMARY purpose of data classification?
A. To select encryption technology
B. To ensure integrity of data
C. To provide a basis for protecting data
D. To determine access rights to data
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Relying on which of the following methods when detecting new threats using IDS should be of MOST concern?
A. Statistical pattern recognition
B. Heuristic analysis
C. Attack signatures
D. Traffic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 7
In information security governance, the PRIMARY role of the board of directors is to ensure:
A. approval of relevant policies and standards.
B. alignment with the strategic goals of the organization
C. compliance with regulations and best practices
D. communication of security posture to stakeholder*
Answer: (SHOW ANSWER)

NEW QUESTION: 8
An organization establishes an internal document collaboration site. To ensure data confidently of each project group, it is MOST important to:
A. Periodically recertify access rights.
B. Conduct vulnerability assessment

C. Enforce document life cycle management
D. Prohibit remote access to the site
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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 that implemented program controls are effective.
B. Demonstrate that the program enables business activities.
C. Demonstrate an increase in ransomware attacks targeting peer organizations.
D. Demonstrate the readiness of business continuity plans.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
When preparing a disaster recovery plan, which of the following would BEST help in prioritizing the restoration of business systems?

A. System utilization requirements
B. Recovery time objective (RTO)
C. Annual loss expectancy (ALE)
D. Service level agreement (SLA)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
A third-party service provider is developing a mobile app for an organization's customers. Which of the following issues should be of GREATEST concern to the information security management.
A. The mobile app s programmers are all offshore contractors.
B. Software escrow is not addressed in the contract
C. SLAs after deployment are not clearly defined.
D. The contract has no requirement for secure development practices
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?
A. Enhanced forensic analysis
B. Reduced need for manual analysis
C. Improved response time to incidents
D. Improved network protection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
Which of the following would BEST enhance firewall security?
A. Logging of security events
B. Placing the firewall on a screened subnet
C. Providing dynamic address assignment
D. Implementing change-control practices
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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. information security controls that reduce enterprise risk.
C. senior management approval of the information security budgets.
D. improved efficiencies of security operations.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?
A. The information regarding monitored activities becomes stale.
B. The activities being monitored deviate from what is considered normal.
C. The environment is complex.
D. The pattern of normal behavior changes quickly and dramatically.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?
A. Continuous monitoring of An information security risk profile
B. Requiring periodic self-assessments by the provider
C. Ensuring the provider's roles and responsibilities are established
D. Evaluating the provider s security incident response plan
Answer: (SHOW ANSWER)

NEW QUESTION: 17
A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value c*n be mitigated by:
A. using the senders public key to encrypt the message.
B. generating hash output that is the same size as the original message,
C. requiring the recipient to use a different hash algorithm,
D. using a secret key m conjunction with the hash algorithm.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the BEST way to address this situation?
A. Revise the information security strategy to meet executive management's expectations.
B. Escalate noncompliance concerns to the internal audit manager
C. Demonstrate alignment of the information security function with business needs.
D. Report the risk and status of the information security program to the board.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
An organization will be outsourcing mission-critical processes. Which of the following is MOST important to verify before signing the service level agreement (SLA)?
A. The provider has implemented the latest technologies.
B. The provider is widely known within the organization's industry.
C. The provider has been audited by a recognized audit firm.
D. The providers technical staff are evaluated annually.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
When designing an incident response plan to be agreed upon with a cloud computing vendor, including which of the following will BEST help to ensure the effectiveness of the plan?

A. An audit and compliance program
B. Requirements for onsite recovery testing
C. Responsibility and accountability assignments
D. A training program for the vendor staff
Answer: (SHOW ANSWER)

NEW QUESTION: 21

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. incoming traffic filtering.
C. IT security policy dissemination.
D. rate limiting.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which of the following is MOST critical for prioritizing actions in a business continuity plan (BCP)?
A. Risk assessment
B. Business process mapping
C. Business impact analysis (BIA)
D. Asset classification
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which of the following is MOST important for the effectiveness of an incident response function?
A. Enterprise security management system and forensic tools
B. Training of all users on when and how to report
C. Establishing prior contacts with law enforcement
D. Automated modem tracking and reporting tools
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Which of the following is the GREATEST security threat when an organization allows remote access through a virtual private network (VPN)?
A. Attackers could compromise the VPN gateway.
B. Client logins are subject to replay attack.
C. VPN traffic could be sniffed and captured.
D. Compromised VPN clients could impact the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:
A. current and target security state for the business.
B. security program priorities to achieve an accepted risk level.
C. assessed level of security risk at a particular point m time.
D. level of compliance with internal policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
When conducting a post-incident review, the GREATEST benefit of collecting mean time to resolution (MTTR) data is the ability to:
A. verify compliance with the service level agreement (SLA).
B. reduce the costs of future preventive controls.
C. learn of potential areas of improvement
D. provide metrics for reporting to senior management
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which of the following MOST effectively prevents internal users from modifying sensitive data?
A. Acceptable use policies
B. Role-based access controls
C. Network segmentation
D. Multi-factor authentication -
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Internal audit has reported a number of information security issues which are not in compliance with regulatory requirements. What should the information security manager do FIRST?
A. Create a security exception
B. Perform a vulnerability assessment
C. Assess the risk to business operations
D. Perform a gap analysis to determine needed resources
Answer: (SHOW ANSWER)

NEW QUESTION: 29
When developing security standards, which of the following would be MOST appropriate to include?
A. Operating system requirements
B. Inventory management
C. Accountability for licenses
D. Acceptable use of IT assets
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?
A. Risk mitigation strategy
B. IT strategy
C. Recovery strategy

D. Security strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 31
The frequency of conducting business impact analysis (BIA) should PRIMARILY be based on:
A. changes in business processes.
B. changes in regulatory requirements.
C. the number of security incidents.
D. business continuity plan (BCP) testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following would provide the BEST justification for a new information security investment?
A. Projected reduction in risk
B. Senior management involvement in project prioritization
C. Defined key performance indicators (KPIs)
D. Results of a comprehensive threat analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following is MOST helpful when justifying the funding required for a compensating control?
A. Risk analysis
B. Business case
C. Threat assessment
D. Business impact analysis (B1A)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
Which of the following is the BEST way to ensure the effectiveness of a role-based access scheme?

A. Review the number of exceptions granted.
B. Implement centralized event logging.
C. Implement a self-service password system.
D. Review the number of unauthorized access attempts.
Answer: (SHOW ANSWER)

NEW QUESTION: 35
The BEST way to improve the effectiveness of responding to and communicating security incidents is to ensure:
A. the IT budget includes funding for SIEM tools to log incidents.
B. senior management is notified at the onset of incident response.
C. the incident response plan is regularly tested.
D. additional staff are trained and available to assist with incident response.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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. Conduct information security awareness training.
C. Create a data classification policy.
D. Implement role-based access controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following provides the MOST relevant evidence of incident response maturity?
A. Average incident closure time
B. Red team testing results
C. Independent audit assessment
D. Tabletop exercise results
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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 risk indicators (KRIs)
B. Critical success factors (CSFs)
C. Key performance indicators (KPIs)
D. Capability maturity models
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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. Benchmark with similar mobile applications to identify gaps
B. Escalate non-implementation of the policy to senior management
C. Analyze the risk and impact of not implementing the policy.
D. Develop and implement a password policy for d mobile application
Answer: (SHOW ANSWER)

NEW QUESTION: 40
In which of the following situations is it MOST important to escalate an incident response to senior management?

A. The time-related service levels for response are below risk threshold levels.
B. The owner of the affected business function is not available.
C. The incident impacts a business-critical system.
D. The impact of the incident exceeds the organization's risk tolerance.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
An information security manager learns of a new international standard related to information security. Which of the following would be the BEST course of action?
A. Determine whether the organization can benefit from adopting the new standard.
B. Review industry peers responses to the new standard.
C. Perform a gap analysis between the new standard and existing practices.
D. Consult with legal counsel on the standard's applicability to regulations
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which of the following is the PRIMARY objective of implementing an information security strategy?
A. To align with industry best practices
B. To maintain adherence to information security policies
C. To manage risk to an acceptable level
D. To demonstrate compliance with legal requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which of the following BEST enables an effective escalation process within an incident response program?

A. Monitored program metrics
B. Defined incident thresholds
C. Dedicated funding for incident management
D. Adequate incident response staffing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following is the BEST way to increase the visibility of information security within an organization's culture?
A. Implementing user awareness campaigns for the entire company
B. Publishing an acceptable use policy
C. Establishing security policies based on industry standards
D. Requiring cross-functional information security training
Answer: (SHOW ANSWER)

NEW QUESTION: 45
When training an incident response team, the advantage of using tabletop exercises is that they:
A. remove the need to involve senior managers in the response process
B. enable the team to develop effective response interactions
C. ensure that the team can respond to any incident
D. provide the team with practical experience in responding to incidents
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?
A. Molding periodic meetings with business owners
B. Creating communication channels
C. Promoting security training
D. Establishing a steering committee
Answer: (SHOW ANSWER)

NEW QUESTION: 47
A global organization is developing an incident response team (IRT). The organization wants to keep headquarters informed of aP incidents and wants to be able to present a unified response to widely dispersed events. Which of the following IRT models BEST supports these objectives?
A. Distributed IRT
B. Holistic IRT
C. Coordinating IRT
D. Central IRT
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which of the following is the MOST important part of an incident response plan?
A. Business impact analysis (BIA)
B. Mean time to report (MTR)
C. Recovery point objective (RPO)
D. Recovery time objective (RTO)
Answer: (SHOW ANSWER)

NEW QUESTION: 49
The MOST important reason to use a centralized mechanism to identify information security incidents is to:
A. detect threats across environments
B. detect potential fraud
C. comply with corporate policies
D. prevent unauthorized changes to networks
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which of the following is a PRIMARY responsibility of an information security governance committee'
A. Analyzing information security policy compliance reviews
B. Approving the purchase of information security technologies
C. Reviewing the information security strategy
D. Approving the information security awareness training strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?
A. Data custodian
B. Data ownership
C. Data encryption

D. Data monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 52
An information security manager is planning to purchase a mobile device management (MDM) system to manage personal devices used by employees to access corpor Which of the following is MOST important to include in the business case?
A. Information security-related metrics
B. Identified risks and mitigating controls
C. Cost-benefit analysis
D. Industry best practice benchmarking results
Answer: (SHOW ANSWER)

NEW QUESTION: 53
An organization has determined that one of its web servers has been compromised. Which of the following actions should be taken to preserve the evidence of the intrusion for forensic analysis and potential litigation?
A. Reboot the server in a secure area to search for digital evidence.
B. Restrict physical and logical access to the server.
C. Run analysis tools to detect the source of the intrusion.
D. Unplug the server from the power.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
An organization is MOST at risk from a new worm being introduced through the intranet when:
A. executable code is run from inside the firewall
B. desktop virus definition files are not up to date
C. system software does not undergo integrity checks.
D. hosts have static IP addresses.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
Reviewing which of the following would provide the GREATEST Input to the asset classification process?
A. Sensitivity of the data
B. Compliance requirements
C. Risk assessment
D. Replacement cost of the asset
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56

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

A. Update the incident response plan.

B. Perform a root cause analysis.

C. Implement compensating controls.

D. Conduct a lessons learned exercise.

Answer: (SHOW ANSWER)

NEW QUESTION: 57

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: 58

Which of the following is MOST helpful in integrating information security governance with corporate governance?

A. Including information security processes within operational and management processes

B. Assigning the implementation of information security governance to the steering committee

C. Aligning the information security governance to a globally accepted framework

D. Providing independent reports of information security efficiency and effectiveness to the board

Answer: (SHOW ANSWER)

NEW QUESTION: 59

Which of the following is the MOST effective way to detect social engineering attacks?

A. Implement an acceptable use policy.

B. Encourage staff to report any suspicious activities.

C. Implement real-time monitoring of security-related events.

D. Provide incident management training to all start.

Answer: (SHOW ANSWER)

NEW QUESTION: 60

An information security manager is concerned that executive management does not su the following is the BEST way to address this situation?

A. Demonstrate alignment of the information security function with business needs.

B. Escalate noncompliance concerns to the internal audit manager

C. Revise the information security strategy to meet executive management expectations.

D. Report the risk and status of the information security program to the board.

Answer: (SHOW ANSWER)

NEW QUESTION: 61
A core business unit relies on an effective legacy system that does not meet the current security standards and threatens that enterprise network. Which of the following is the BEST course of action to address the situation?
A. Develop processes to compensate for the deficiencies.
B. Require that new systems that can meet the standards be implemented.
C. Disconnect the legacy system from the rest of the network.
D. Document the deficiencies in the risk register.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?
A. Test incident response procedures regularly.
B. Obtain senior management commitment
C. Communicate incident response procedures to staff.
D. Establish and measure key performance indicators (KPIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Senior management commitment and support will MOST likely be offered when the value of information security governance is presented from a:
A. risk perspective.
B. policy perspective.
C. threat perspective.
D. compliance perspective
Answer: (SHOW ANSWER)

NEW QUESTION: 64

Which of the following should an information security manager establish FIRST to ensure security-related activities are adequately monitored?
A. Accountability for security functions
B. Regular reviews of computer system logs
C. Internal reporting channels
D. Scheduled security assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 65
A new privacy regulation is due to take effect in a region where an organization does business. Which of the following would be MOST helpful in understanding what .. needs to do to maintain compliance?
A. Vulnerability assessment
B. Internal audit review
C. Legal department review
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Risk identification, analysis, and mitigation activities can BCST be integrated into business life cycle processes by linking them to:
A. continuity planning
B. compliance testing
C. configuration management.
D. change management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 67
Which of the following would BEST help to ensure an organization's information security strategy is aligned with business objectives?
A. Requesting senior management to periodically review security incidents
B. Implementing an automated solution for monitoring information security processes
C. Establishing metrics to measure the effectiveness of the information security program
D. Establishing a change control process for continued updating of security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following is MOST critical for the successful implementation of an information security strategy?
A. Ongoing commitment from senior management
B. Established information security policies

C. Compliance with regulations
D. Sizeable funding for the information security program
Answer: (SHOW ANSWER)

NEW QUESTION: 69
An organization's information security manager will find it MOST difficult to perform a post-incident review of a data leakage event when it is related to:
A. outsourced service providers
B. public cloud services
C. corporate mobile devices,
D. private cloud services.
Answer: (SHOW ANSWER)

NEW QUESTION: 70
In an organization implementing a data classification program, ultimate responsibility for the data on the database server lies with the:

A. business unit manager
B. information technology manager.
C. information security manager.
D. database administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Which of the following will BEST ensure that risk is evaluated on system level changes?
A. System development staff receives regular security training.
B. Senior management must sign-off on changes.
C. Implement a centralized change management system.
D. Security should be integrated in the change control process.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Conducting a cost-benefit analysis for a security investment is important because it
A. quantifies return on security investment
B. supports asset classification.
C. quantifies residual risk
D. supports justification for expenditure.
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following would BEST help an information security manager prioritize remediation activities to meet regulatory requirements?

A. Annual toss expectancy (ALE) of noncompliance
B. Cost of associated controls
C. A capability maturity model matrix
D. Alignment with the IT strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 74
An organization plans to implement a document collaboration solution to allow employees to share company information. Which of the following is the MOST important control to mitigate the risk associated with the new solution?
A. Assign write access to data owners.
B. Allow a minimum number of users access to the solution.
C. Permit only non-sensitive information on the solution.
D. Have data owners perform regular user access reviews.
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following is the BEST way for an information security manager to promote the integration of information security considerations into key business processes?
A. Provide information security awareness training.
B. Facilitate the creation of an information security steering group
C. Conduct information security briefings for executives
D. Conduct a business impact analysis (BIA).
Answer: (SHOW ANSWER)

NEW QUESTION: 76
To gain a clear+ understanding of the impact that a new regulatory requirement will have on an organization s information security controls, an information security manager should FIRST:
A. perform a gap analysis.
B. conduct a risk assessment
C. interview senior management
D. conduct a cost-benefit analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which of the following would BEST enable an organization to effectively monitor the implementation of standardized configurations?
A. Perform periodic audits to detect non-com pliant configurations.
B. Develop policies requiring use of the established benchmarks.
C. Implement automated scanning against the established benchmarks.
D. Implement a separate change tracking system to record changes to configurations.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following would be of GREATEST concern to an information security manager when evaluating a cloud service provider (CSP)?
A. Data retention policies may be violated.
B. Security controls offered by the provider are inadequate
C. Service level agreements (SLAs) art not well defined.
D. There is no right to audit the security of the provider
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Which of the following will BEST enable an effective information asset classification process?
A. Including security requirements in the classification process
B. Reviewing the recovery time objective (RTO) requirements of the asset
C. Analyzing audit findings
D. Assigning ownership
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
Which of the following is an example of a vulnerability?
A. Unauthorized users
B. Natural disasters
C. Ransomware
D. Defective software
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?
A. Identifying the threat environment
B. Identifying risk mitigation options

C. Identifying critical business processes
D. Identifying key business risks
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which of the following is the PRIMARY product of a business impact analysis (BIA)?
A. Prioritization of vulnerabilities for remediation
B. Well-defined incident escalation procedures
C. A heat map of business risk scenarios
D. Prioritization of assets for business recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following would be MOST helpful in gaining support for a business case for an information security initiative?
A. Presenting a solution comparison matrix
B. Referencing control deficiencies
C. Emphasizing threats to the organization
D. Demonstrating organizational alignment
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following should an incident response team do NEXT after validating an event is an incident?
A. Contain the incident.
B. Identify the toot cause.
C. Invoke the response plan.
D. Escalate to management
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which of the following would BEST fulfill a board of directors' request for a concise
A. Balanced scorecard
B. Risk register
C. Business impact analysis
D. Risk heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 86
The PRIMARY advantage of a network intrusion detection system (IDS) is that it can:
A. simulate denial-of-service attacks.

B. identify an attack on the network.
C. detect network vulnerabilities
D. block undesirable network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following threats is prevented by using token-based authentication?
A. Session eavesdropping attack on the network
B. Denial of service attack over the network
C. Password sniffing attack on the network
D. Man-in-the-middle attack on the client
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following is the BEST approach for determining the maturity level of an information security program?
A. Review internal audit results.
B. Evaluate key performance indicators (KPIs).
C. Engage a third-party review.
D. Perform a self-assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Which of the following BEST demonstrates effective information security management within an organization?
A. Information security governance is incorporated into organizational governance.
B. Control ownership is assigned to parties who can accept losses related to control failure.
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: 90
Which of the following is the MOST important characteristic of an effective security policy?
A. The policy provides broad organizational direction.
B. The policy has been validated by business owners.
C. The policy includes actionable procedures.
D. The policy is aligned to industry best practice.
Answer: (SHOW ANSWER)

NEW QUESTION: 91

What information is MOST helpful in demonstrating to senior management how information security governance aligns with business objectives?
A. A list of monitored threats, risks and exposures
B. Updates on information security projects in development
C. Drafts of proposed policy changes
D. Metrics of key information security deliverables
Answer: (SHOW ANSWER)

NEW QUESTION: 92
When developing a classification method for incidents, the categories MUST be:
A. assigned to incident handlers.
B. regularly reviewed.
C. quantitatively defined.
D. specific to situations.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
A system administrator failed to report a security incident where the critical application server was not available to the business users. Which of the following is the BEST way to prevent a reoccurrence?
A. Document the incident response plan
B. Communicate disciplinary procedures.
C. Conduct incident response plan testing.
D. Define communication processes
Answer: (SHOW ANSWER)

NEW QUESTION: 94
A multinational organization wants to ensure its privacy program appropriately addresses privacy risk throughout its operations. Which of the following would be of MOST concern to senior management?
A. The organization doe* not have a dedicated privacy officer
B. Privacy policies ire only reviewed annually

C. The organization uses a decentralized privacy governance structure
D. The privacy program does not include a formal warning component
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Application data integrity risk would be MOST directly addressed by a design that includes:
A. access control technologies such as role-based entitlements.
B. strict application of an authorized data dictionary.
C. reconciliation routines such as checksums, hash totals, and record counts
D. application log requirements such as field-level audit trails and user activity logs.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
Which of the following is the PRIMARY role of a data custodian?
A. Securing information
B. Validating information
C. Processing information
D. Classifying information
Answer: (SHOW ANSWER)

NEW QUESTION: 97
After a risk has been mitigated, which of the following is the BEST way to help ensure residual risk remains within an organization's established risk tolerance?
A. Perform a business impact analysis (BIA).
B. Introduce new risk scenarios to test program effectiveness.
C. Conduct programs to promote user risk awareness
D. Monitor the security environment for changes in risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Business impact analysts
B. Annual risk assessments
C. Security baselining
D. Continuous monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 99
The PRIMARY role of an information security steering group is to ensure that:
A. there is compliance with software-copyright legislation.

B. security procedures and practices are in line with formal policies.
C. security policies address business issues.
D. there is compliance with security standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 100
The MOST important reason that security risk assessments should be conducted frequently throughout an organization is because:

A. threats to the organization may change.
B. compliance with legal and regulatory standards should be reassessed.
C. controls should be regularly tested.
D. control effectiveness may weaken.
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Which of the following is the MOST important reason for performing a risk analysis?
A. Identifying critical information assets
B. Assigning the appropriate level of protection
C. Promoting increased security awareness in the organization
D. Identifying and eliminating threats
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following is the GREATEST benefit of information asset classification to an organization?
A. It demonstrates the value of information assets for financial reporting.
B. It helps to optimize the investment in protecting information assets.
C. It measures qualitative value of the information.
D. It helps to minimize the cost of regulatory compliance efforts
Answer: (SHOW ANSWER)

NEW QUESTION: 103
The MOST effective way to continuously monitor an organization's cybersecurity posture is to evaluate its
A. key performance indicators (KPIs).
B. compliance with industry regulations.
C. level of support from senior management.
D. timeliness m responding to attacks.
Answer: (SHOW ANSWER)

NEW QUESTION: 104

When making an outsourcing decision, which of the following functions is MOST important to retain within the organization?
A. Incident response
B. Risk assessment
C. Security management
D. Security governance
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following is the MOST relevant source of information for determining the available internal human resources for executing the information security program?
A. RACI chart
B. Job descriptions
C. Skills inventory
D. Roles and responsibilities matrix
Answer: C (LEAVE A REPLY)

NEW QUESTION: 106
Which of the following BIST validates that security controls are implemented in a new business process?
A. Review the process for conformance with information security best practices
B. Benchmark the process against industry practices
C. Verify the use of a recognized control framework
D. Assess the process according to information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 107
When determining an acceptable risk level, which of the following is the MOST important consideration?
A. Threat profile
B. Vulnerability scores
C. Risk matrices

D. System criticality
Answer: (SHOW ANSWER)

NEW QUESTION: 108
A large organization is considering a policy that would allow employees to briog their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:
A. impact on network capacity.
B. lack of a device management solution.
C. higher costs in supporting end users.
D. decrease in end user productivity.
Answer: (SHOW ANSWER)

NEW QUESTION: 109
What is a potential issue when emails are encrypted and digitally signed?
A. The receiver can repudiate the receipt of the emails.
B. Hackers can eavesdrop on emails.
C. Hackers can introduce forged messaging within emails.
D. The sender can repudiate the contents of the emails.
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following is MOST important for an information security manager to communicate to senior management regarding the security program?

A. Impact analysts results
B. User roles and responsibilities
C. Potential risks and exposures
D. Security architecture changes
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which of the following would present the GREATEST need to revise information security poll'
A. Changes in standards and procedures
B. A merger with a competing company
C. Implementation of a new firewall
D. An increase in reported incidents
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
Which of the following is an information security manager's BEST course of action upon identification of a shadow IT application being used by a business unit?

A. Report the application to the IT department.
B. Notify senior management of the application.
C. Perform a vendor due diligence review.
D. Determine the nature of information within the application.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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. Internal audit
C. The steering committee
D. The legal department
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which of the following circumstances would MOST likely require a review and update to an organization's information security incident response plan?
A. A new business strategy has been developed.
B. A high-risk vulnerability has been detected.
C. The organizational structure has changed.
D. A new business application has been implemented.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following is MOST important to the successful implementation of an information security governance framework across the organization?
A. Security policies that adhere to industry best practices
B. Security management processes aligned with security objectives
C. The existing organizational security culture
D. Organizational security controls deployed in line with regulations
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following is MOST important when selecting an information security metric?
A. Ensuring the metric is repeatable
B. Defining the metric in quantitative terms
C. Aligning the metric to the IT strategy
D. Defining the metric in qualitative terms
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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 most stringent requirements.
C. international security standards.
D. the security organization structure
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which of the following provides the BEST indication that the information security program is in alignment with enterprise requirements?
A. The information security manager reports to the chief executive officer.
B. The security strategy is benchmarked with similar organizations
C. Security strategy objectives are defined in business terms.
D. An IT governance committee is m place.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
Which of the following is the MOST important consideration when designing information security architecture?
A. The existing threat landscape is monitored.
B. The level of security supported is based on business decisions.
C. Risk management parameters for the organization are defined.
D. The information security architecture is aligned with industry standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which of the following is the MOST important step in risk ranking?
A. Threat assessment
B. Vulnerability analysis
C. Mitigation cost
D. Impact assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 121
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: 122
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 an analysis of current risk exposures.
C. Provide the estimated return on investment (ROI).
D. Include industry benchmarking comparisons.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following should be the PRIMARY expectation of management when an organization introduces an information security governance framework?
A. Increased influence of security management
B. Consistent execution of information security strategy
C. Optimized information security resources
D. Improved accountability to shareholders
Answer: (SHOW ANSWER)

NEW QUESTION: 124
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 governance framework
B. Cloud security strategy
C. Risk assessment
D. Vulnerability assessment

Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which of the following would provide nonrepudiation of electronic transactions?
A. Periodic reaccredinations
B. Two-factor authentication
C. Third-party certificates
D. Receipt acknowledgment
Answer: (SHOW ANSWER)

NEW QUESTION: 126
A risk has been formally accepted and documented. Which of the following is the MOST important action for an information security manager?
A. Monitor the environment for changes
B. Update risk tolerance levels.
C. Notify senior management and the board.
D. Re-evaluate the organization's risk appetite
Answer: (SHOW ANSWER)

NEW QUESTION: 127
A business unit has updated its long-term business plan to include a strategy of upgrading information management systems to increase productivity. To support this initiative, what should be the PRIMARY basis for updating the corresponding. information security strategy?
A. The IT strategy
B. The business strategy
C. IT risk assessment results
D. The information security framework
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following is the KST way to align security and business strategies?
A. Include security risk as part of corporate risk management,
B. Integrate information security governance into corporate governance
C. Establish key performance indicators (KPIs) for business through security processes.
D. Develop a balanced scorecard for security
Answer: D (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following is MOST effective in the strategic alignment of security initiatives?
A. Business leaders participate in information security decision making
B. Policies are created with input from business unit managers.

C. A security steering committee is set up within the IT deployment.
D. Key information security policy are updated on a regular basis
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following would BEST assist an information security manager in gaining strategic support from executive management?

A. Risk analysis specific to the organization
B. Research on trends in global information security breaches
C. Annual report of security incidents within the organization
D. Rating of the organization s security, based on international standards
Answer: (SHOW ANSWER)

NEW QUESTION: 131
Which of the following should be the PRIMARY input when defining the desired state of security within an organization?
A. Level of business impact
B. Annual loss expectancy
C. Acceptable risk level
D. External audit results
Answer: (SHOW ANSWER)

NEW QUESTION: 132
The use of a business case to obtain funding for an information security investment is MOST effective when the business case:
A. relates the investment to the organization's strategic plan.
B. articulates management s intent and information security directives in clear language.
C. realigns information security objectives to organizational strategy,
D. translates information security policies and standards into business requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
Which of the following would provide the MOST useful input when creating an information security program?
A. Information security budget
B. Information security strategy
C. Business case
D. Key risk indicators (KRIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 134

An information security manager is reviewing the impact of a regulation on the organization's human resources system. The NEXT course of action should be to:
A. review the organization's most recent audit report.
B. determine the cost of compliance.
C. assess the penalties for non-compliance.
D. perform a gap analysis of compliance requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Which of the following is the BEST criterion to use when classifying assets?
A. The market value of the assets
B. Value of the assets relative to the organization
C. Recovery time objective (RTO)
D. Annual loss expectancy (ALE)
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following is MOST important for an information security manager to consider when developing a new information security policy?
A. Information security budget allocation
B. Organizational culture and complexity
C. Organizational goals and objectives
D. Alignment with industry standards
Answer: (SHOW ANSWER)

NEW QUESTION: 137
When facilitating the alignment of corporate governance and information security governance, which of the following is the MOST important role of an organizations security steering committee?
A. Obtaining support for the integration from business owners
B. Defining metrics to demonstrate alignment
C. Evaluating and reporting the degree of integration

D. Obtaining approval for the information security budget
Answer: (SHOW ANSWER)

NEW QUESTION: 138
To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:
A. the security policy is changed to accommodate IT performance pressure
B. senior management provides guidance and dispute resolution
C. noncompliance issues are reported to senior management
D. information security management understands business performance issues
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?
A. Gap analysis
B. impact analysis (BIA)
C. Risk assessment
D. Business
E. Penetration resting
Answer: (SHOW ANSWER)

NEW QUESTION: 140
An information security manager has identified numerous violations of security policy which prohibits text messaging from personal devices to conduct official business following is the MOST effective way to reduce the number of violations?

A. Report violations to senior management.
B. Provide awareness training to end users.
C. Implement a mobile device management (MDM) solution.
D. Require management approval for policy exceptions.
Answer: (SHOW ANSWER)

NEW QUESTION: 141
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. Prioritize security controls based on risk.
B. Suggest less expensive alternative security controls.
C. Request a budget exception for the security controls
D. Begin the risk acceptance process
Answer: (SHOW ANSWER)

NEW QUESTION: 142
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. Perform root cause analysis.
C. Update the risk register.
D. Invoke the incident response plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
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
A. Selecting the virtualization software
B. Ensuring the project has appropriate security funding
C. Determining how incidents will be managed
D. Being involved at the design stage of the project
Answer: (SHOW ANSWER)

NEW QUESTION: 144
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 must be stored in an encrypted format on the mobile device
B. A senior manager must approve each new connection
C. Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
D. Users must agree to allow the mobile device to be wiped if it is lost
Answer: (SHOW ANSWER)

NEW QUESTION: 145
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. Providing annual awareness training regarding incident response for team members
B. Rehearsing incident response procedures rote, and responsibilities
C. Validating the incident response plan against industry best practices
D. Defining modern seventy levels during a business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 146
BEST way to isolate corporate data stored on employee-owned mobile devices would be to implement:
A. a strong password policy
B. two-factor authentication

C. device encryption,
D. a sandbox environment
Answer: (SHOW ANSWER)

NEW QUESTION: 147
An information security program should be established PRIMARILY on the basis of:
A. senior management input
B. data security regulatory requirements.
C. the approved information security strategy.
D. the approved risk management approach.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?
A. Compliance requirements associated with the regulation
B. Compensating controls in place to protect information security
C. Corresponding breaches associated with each vendor
D. Criticality of the service to the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 149
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. Perform a risk assessment
B. Design and document a new process
C. Update the security policy
D. Report the issue to senior management
Answer: (SHOW ANSWER)

NEW QUESTION: 150
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. Limit access to the third-party contractor
C. Terminate the agreement with the third-party contractor
D. Include security requirements in outsourcing contracts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 151
An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST"
A. Data owners
B. Communications department
C. Application owners
D. Security operations team
Answer: (SHOW ANSWER)

NEW QUESTION: 152
Which of the following will BEST help to ensure security is addressed when developing a custom application?
A. Conducting security training for the development staff
B. Integrating a security audit throughout the development process
C. Integrating security requirements into the development process
D. Requiring a security assessment before implementation
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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. Apply the current corporate security policies to the new office.
B. Identify applicable regulatory requirements to establish security policies
C. Update privacy policies to include the other country's laws and regulations.
D. Encrypt the data for transfer to the head office based on security manager approval
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which of the following BEST demonstrates that an organization supports information security governance?
A. Employees attend annual organization-wide security training.

B. The incident response plan is documented and tested regularly.
C. Information security steering committee meetings are held regularly.
D. Information security policies are readily available to employees.
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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: D (LEAVE A REPLY)

NEW QUESTION: 156
Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?
A. Capability of online virtual machine analysis
B. Availability of current infrastructure documentation
C. Capability to take a snapshot of virtual machines
D. Availability of web application firewall logs
Answer: (SHOW ANSWER)

NEW QUESTION: 157
Which of the following activities should take place FIRST when a security patch for Internet software is received from a vendor?
A. The patch should be deployed quickly to systems that are vulnerable.
B. The patch should be validated using a hash algorithm.
C. The patch should be evaluated in a testing environment.
D. The patch should be applied to critical systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Which of the following BEST demonstrates alignment between information security governance and corporate governance?
A. Number of vulnerabilities identified for high-risk information assets
B. Security project justifications provided in terms of business value
C. Mean time to resolution for enterprise-wide security incidents
D. Average number of security incidents across business units
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Risk management is MOST cost-effective;
A. when integrated into other corporate assurance functions.
B. while developing the business case for the security program
C. at the beginning of security program development
D. when performed on a continuous basis.
Answer: (SHOW ANSWER)

NEW QUESTION: 160
It is MOST important tot an information security manager to ensure that security risk assessments are performed:

A. during a root cause analysis
B. consistently throughout the enterprise.
C. In response to the threat landscape,
D. as part of the security business case
Answer: (SHOW ANSWER)

NEW QUESTION: 161
When determining an acceptable risk level, which of the following is the MOST important consideration?
A. Risk matrices
B. System criticality
C. Vulnerability scores
D. Threat profile
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
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. Implement a mobile device management solution.
C. Document a bong-your-own-device (BYODJ policy.
D. implement a multi-factor authentication solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following should be the FIRST step of incident response procedures?
A. Identify if there is a need for additional technical assistance.
B. Evaluate the cause of the control failure.
C. Classify the event depending on seventy and type.

D. Perform a risk assessment to determine the business impact.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 164
Which of the following BEST reduces the likelihood of leakage of private information via email?
A. Email encryption
B. Strong user authentication protocols
C. User awareness training
D. Prohibition on the personal use of email
Answer: (SHOW ANSWER)

NEW QUESTION: 165
In a resource-restricted security program, which of the following approaches will provide the BEST use of the limited resources?
A. Risk avoidance
B. Cross-training
C. Threat management
D. Risk prioritization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166
Failure to include information security requirements within the build/buy decision would MOST likely result in the need for:
A. commercial product compliance with corporate standards.
B. more stringent source programming standards.
C. compensating controls in the operational environment.
D. security scanning of operational platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 167
A company has purchased a rival organization and is looking to integrate security strategies. Which of the following is the GREATEST issue to consider?

A. Confidential information could be leaked
B. Differing security technologies
C. The organizations have different risk appetites
D. Differing security skills within the organizations
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Senior management has allocated funding to each of the organization s divisions to address information security vulnerabilities The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?
A. Redundant controls may be implemented across divisions.
B. Information security governance could be decentralized by division.
C. Return on investment may be inconsistently reported to senior management
D. Areas of highest risk may not be adequately prioritized for treatment.
Answer: (SHOW ANSWER)

NEW QUESTION: 169
For a user of commercial software downloaded from the Internet, which of the following is the MOST effective means of ensuring authenticity?
A. Digital certificates
B. Digital code signing
C. Digital signatures
D. Steganography
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Which of the following is the BEST way to rigorously test a disaster recovery plan for a mission-critical system without disrupting business operations?

A. Simulation testing
B. Parallel testing
C. Checklist review
D. Structured walk-through
Answer: (SHOW ANSWER)

NEW QUESTION: 171
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. A damage assessment expert for calculating losses
B. A forensics expert for evidence management
C. An independent auditor for identification of control deficiencies

D. A penetration tester to validate the attack
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?
A. The vendor's reputation m the industry
B. The ability to meet deliverables
C. The business need for the function
D. The cost of the services
Answer: (SHOW ANSWER)

NEW QUESTION: 173
What is the BEST way for an information security manager to maintain continuous insight into the effectiveness of the organization's information security program?
A. Develop timely information security risk reporting.
B. Establish information security metrics.
C. Solicit feedback from end users
D. Conduct quarterly penetration testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 174
The PRIMARY purpose of asset valuation for the management of information security is to:
A. provide a basis for asset classification.
B. eliminate the least significant assets.
C. determine the value of each asset
D. prioritize risk management activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which of the following would provide senior management with the BEST overview of the performance of information security risk treatment options?
A. Before-and-after heat maps
B. individual risk assessments
C. Detailed risk analysis of the treatments
D. Analysis of recent incident
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Calculation of the recovery time objective (RTO) is necessary to determine the:
A. annual loss expectancy (ALE)

B. point of synchronization
C. time required to restore files.
D. priority of restoration.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
The MOST likely cause of a security information event monitoring (SIEM) solution failing to identify a serious incident is that the system:
A. is not collecting logs from relevant devices.
B. has performance issues
C. has not been updated with the latest patches
D. is hosted by a cloud service provider
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which of the following is the MOST effective approach for integrating security into application development?
A. Including security in user acceptance testing sign-off
B. Developing security models in parallel
C. Defining security requirements
D. Performing vulnerability scans
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Web application firewalls are needed in addition to other intrusion prevention and detection technology PRIMARILY because:
A. they recognize web application protocols.
B. they prevent modification of application source code
C. web services are prone to attacks.
D. web services require unique forensic evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 180
A contract bid is digitally signed and electronically mailed The PRIMARY advantage to using a digital signature is that

A. the bid cannot be forged even if the keys are compromised.
B. any alteration of the bid will invalidate the signature.
C. the bid and the signature can be copied from one document to another
D. the signature can be authenticated even if no encryption is used,
Answer: (SHOW ANSWER)

NEW QUESTION: 181
Which of the following would BEST help to ensure compliance with an organizations information security requirements by an IT service provider?
A. Requiring regular reporting from the IT service provider
B. Requiring an external security audit of the IT service provider
C. Defining information security requirements with internal IT
D. Defining the business recovery plan with the IT service provider
Answer: (SHOW ANSWER)

NEW QUESTION: 182
Which of the following is the MOST important element of a response plan for IT security incidents?
A. Requirements for investigative evidence
B. Appropriate team members
C. Test plans for containment and recovery procedures
D. Guidelines for preserving digital evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 183
When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?
A. Encryption
B. Retention
C. Tuning
D. Report distribution
Answer: (SHOW ANSWER)

NEW QUESTION: 184
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. Conduct security testing

B. Require device encryption
C. Develop a personal device policy
D. Assess the security risk
Answer: (SHOW ANSWER)

NEW QUESTION: 185
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: 186
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. Regulatory requirements
C. Cost to remediate
D. Risk treatment options
Answer: (SHOW ANSWER)

NEW QUESTION: 187
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: 188
Which of the following is the BIST course of action for the information security manager when residual risk is above the acceptable level of risk?
A. Perform a cost-benefit analysis.
B. Defer to business management.
C. Recommend additional controls.
D. Carry out a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 189
Which of the following would provide the MOST helpful information when developing a prioritized list of IT assets to protect in the event of an incident?
A. The service level agreement (SLA) for the IT asset
B. The replacement cost of the IT asset
C. The classification of the information processed by the IT asset
D. The owner of the IT asset
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following is the PRIMARY driver of information security compliance?
A. Threat environment
B. Regulatory requirements
C. Industry standards
D. Risk appetite
Answer: (SHOW ANSWER)

NEW QUESTION: 191
Which of the following enables compliance with a nonrepudiation policy requirement for electronic transactions?
A. Digital certificates
B. Digital signatures
C. Encrypted passwords
D. One-time passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 192
In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?
A. Conduct a business impact analysis (BIA) and provide the report to management
B. Stop providing mobile devices until the organization is able to implement controls.
C. Include the topic of prohibited texting in security awareness training.
D. Update the corporate mobile usage policy to prohibit texting.
Answer: (SHOW ANSWER)

NEW QUESTION: 193
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. Create a business case appeal decision.
B. Prioritize security projects based on risk.
C. Design key risk indicators (KRIs)

D. Remove overlapping security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 194
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. Business objectives and related IT risk
C. Industry best practices applicable to the business
D. Government regulations and related penalties
Answer: (SHOW ANSWER)

NEW QUESTION: 195
A validated patch to address a new vulnerability that may affect a mission-critical server has been released. What should be done immediately?
A. Add mitigating controls.
B. Conduct an impact analysis.
C. Check the server s security and install the patch.
D. Take the server off-line and install the patch.
Answer: (SHOW ANSWER)

NEW QUESTION: 196
What is the GREATEST benefit of classifying assets based on sensitivity?
A. The organization can allocate appropriate levels of protection.
B. Staff can create more realistic risk scenarios.
C. The organization is in compliance with regulatory guidelines.
D. Data is available to appropriately assign asset ownership.
Answer: (SHOW ANSWER)

NEW QUESTION: 197
A business unit uses e-commerce with a strong password policy. Many customers complain that they cannot remember their password because they are too long and complex. The business unit

states it is imperative to improve the customer experience. The information security manager should FIRST.

A. Reach alternative secure of identify verification

B. Recommended implementing two-factor authentication.

C. Change the password policy to improve the customer experience

D. Evaluate the impact of the customer's experience on business revenue.

Answer: (SHOW ANSWER)

NEW QUESTION: 198

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

A. when multiple sessions with the same application ID collide, the database locks up

B. the database becomes unavailable if the password of The application ID expires.

C. users can gam direct access to the application ID and circumvent data controls,

D. an incident involving unauthorized access to data cannot be tied to a specific user

Answer: (SHOW ANSWER)

NEW QUESTION: 199

Which of the following is the BEST indication that a recently adopted information security framework is a good fit for an organization?

A. The framework includes industry-recognized information security best practices.

B. The business has obtained framework certification.

C. Objectives in the framework correlate directly to business practices

D. The number of security incidents has significantly declined

Answer: (SHOW ANSWER)

NEW QUESTION: 200

Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

A. Updating information security awareness materials

B. Providing ongoing training to the incident response team

C. Implementing a honeypot environment

D. Implementing proactive systems monitoring

Answer: A (LEAVE A REPLY)

NEW QUESTION: 201

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

A. Eradication

B. Containment

C. Identification
D. Review
Answer: (SHOW ANSWER)

NEW QUESTION: 202
Which of the following provides the BEST justification for an information security investment when creating a business case
A. The investment reduces the protected asset s inherent risk below the asset s residual risk
B. The investment can be managed using the organisation's established system development life cycle.
C. Key risk indicators (KRIs) are available to measure the effectiveness and efficiency of the investment
D. The annualized loss expectancy (ALE) is greater than the annual cost of the investment.
Answer: (SHOW ANSWER)

NEW QUESTION: 203
A risk profile supports effective security decisions PRIMARILY because it:
A. enables comparison with industry best practices.
B. describes security threats.
C. defines how to best mitigate future risks.
D. identifies priorities for risk reduction.
Answer: (SHOW ANSWER)

NEW QUESTION: 204
When supporting a large corporation's board of directors in the development of governance, which of the following is the PRIMARY function of the information security manager?
A. Preparing the security budget
B. Gaining commitment of senior management
C. Developing a balanced scorecard
D. Providing advice and guidance
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Senior management learns of several web application security incidents and wants to know the exposure risk to the organization. What is the information security manager's BEST course of action?
A. Assess IT system configurations
B. Review audit logs from IT systems.
C. Activate the incident response plan
D. Perform a vulnerability assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which of the following is a PRIMARY objective of incident classification?
A. Increasing response efficiency
B. Enabling incident reporting
C. Complying with regulatory requirements
D. Reducing escalations to management
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following is the MOST effective way to detect security incidents?
A. Analyze vulnerability assessments.
B. Analyze recent security risk assessments.
C. Analyze penetration test results.
D. Analyze security anomalies.
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Which of the following is the BEST way to prevent employees from making unauthorized comments to the media about security incidents in progress?
A. Establish standard media responses for employees to control the message
B. Communicate potential disciplinary actions for noncompliance.
C. training Implement controls to prevent discussion with media during an Incident.
D. Include communication policies In regular information security training
Answer: (SHOW ANSWER)