ISACA.CISM.v2020-09-08.q255

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	255
Version:	v2020-09-08
# of views:	2047
# of Questions views:	95692
https://www.freecram.net/torrent/ISACA.CISM.v2020-09-08.q255.html	

NEW QUESTION: 1
The MOST effective way to communicate the level of impact of information security risks on organizational objectives is to present
A. risk treatment options.
B. detailed threat analysis results.
C. business impact analysis (BIA) results.
D. a risk heat map.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following would be an information security manager's PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?
A. Disparate device security
B. Mobile application control
C. End user acceptance
D. Configuration management
Answer: (SHOW ANSWER)

NEW QUESTION: 3
A recent phishing attack investigation showed that several employees had used their work email addresses to create personal accounts on a shopping site that had been breached. What is the BEST way to prevent this
A. Update the incident response plan to address this situation.
B. Block personal shopping sites using proxy filtering.
C. Conduct information security awareness training for employees.
D. Send periodic fake phishing emails to employees and track responses.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?
A. impact analysis (BIA)
B. Gap analysis
C. Business
D. Risk assessment
E. Penetration resting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
Which of the following is the BEST way to determine if an information security program aligns with corporate governance?
A. Review information security policies.
B. Review the balanced scorecard.
C. Evaluate funding for security initiatives.
D. Survey end users about corporate governance.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
An organization is the victim of a targeted attack, and is unaware of the compromise until a security analyst notices an additional user account on the firewall. The implementation of which of the following would have detected the incident?
A. Security information event management (SIEM)
B. Network access control (NAC)
C. Web-application firewall (WAF)
D. Data leakage prevention (OLP)
Answer: (SHOW ANSWER)

NEW QUESTION: 7
A risk profile supports effective security decisions PRIMARILY because it:
A. identifies priorities for risk reduction.
B. enables comparison with industry best practices.
C. describes security threats.
D. defines how to best mitigate future risks.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?

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

NEW QUESTION: 9
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. Utilize multi-factor authentication
B. Utilize encryption for account logins.
C. Create unique login credentials for each user.
D. Rotate account passwords regularly.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
To implement a security framework, an information security manager must FIRST develop:
A. security guidelines
B. security procedures
C. a security policy
D. security standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
The BEST way to establish a recovery time objective (RTO) that balances cost with a realistic recovery time frame is to:
A. perform a business impact analysis (BIA).
B. conduct a risk assessment
C. determine daily downtime cost.
D. analyze cost metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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. Central IRT
B. Distributed IRT
C. Holistic IRT
D. Coordinating IRT

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. Identify the toot cause.
B. Escalate to management
C. Invoke the response plan.
D. Contain the incident.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which of the following is the MOST important factor to consider when establishing a severity hierarchy for information security incidents?
A. Residual risk
B. Business impact
C. Management support
D. Regulatory compliance
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 been audited by a recognized audit firm.
B. The providers technical staff are evaluated annually.
C. The provider is widely known within the organization's industry.
D. The provider has implemented the latest technologies.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of integrity?
A. Ensuring encryption for data in transit
B. Implementing a data classification schema
C. Utilizing a formal change management process
D. Enforcing service level agreements (SLAs)
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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: 18
Reviewing security objectives and ensuring the integration of security across business units is PRIMARILY the focus of the:
A. steering committee.
B. chief information security officer (CISO).
C. board of directors.
D. executive management
Answer: (SHOW ANSWER)

NEW QUESTION: 19
The selection of security controls is PRIMARILY linked to:
A. best practices of similar organizations.
B. regulatory requirements
C. risk appetite of the organization.
D. business impact assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 20
A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the BEST way to obtain assurance that the provider can adequately protect the organization's information?

A. Invoke the right to audit per the contract
B. Review the provider s information security policy.
C. Review the providers serf-assessment

D. Check references supplied by the provider's other customers
Answer: (SHOW ANSWER)

NEW QUESTION: 21
The effectiveness of security awareness programs in fostering positive security cultures is MOST dependent upon employee:
A. awareness of regulatory requirements.
B. understanding of the penalties for noncompliance.
C. ability to carry out security-related procedures.
D. ownership of security responsibilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which of the following is the MOST effective method to prevent a SQL injection in an employee portal?
A. Conduct network penetration testing.
B. Enforce referential integrity on the database.
C. Conduct code reviews.
D. Reconfigure the database schema.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which of the following is MOST important to consider when developing a disaster recovery plan?
A. Business continuity plan (BCP)
B. Cost-benefit analysis
C. Feasibility assessment
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Which of the following is a PRIMARY responsibility of an information security governance committee'
A. Approving the purchase of information security technologies
B. Analyzing information security policy compliance reviews
C. Approving the information security awareness training strategy
D. Reviewing the information security strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 25
During an emergency security incident, which of the following would MOST likely predict the worst-case scenario?

A. Vulnerability assessment report
B. Risk assessment report
C. Cost-benefit analysis report
D. Business impact analysis (B1A) report
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which of the following is the PRIMARY product of a business impact analysis (BIA)?
A. A heat map of business risk scenarios
B. Prioritization of assets for business recovery
C. Prioritization of vulnerabilities for remediation
D. Well-defined incident escalation procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 27
An audit reveals that some of an organizations software is end-of-life and the vendor will no longer provide support or security patches. Which of the following is the BEST way for the information security manager to address this situation?
A. Research compensating security controls.
B. Research alternative software solutions.
C. Assess the risk and impact to the business.
D. Segment the affected system on the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following is the MOST important outcome of testing incident response plans?
A. Internal procedures are improved.
B. Areas requiring investment are identified.
C. An action plan is available for senior management.
D. Staff is educated about current threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following defines the triggers within a business continuity plan (BCP)?
A. Information security policy
B. Disaster recovery plan (DRP)
C. Gap analysis
D. Needs of the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 30

For a user of commercial software downloaded from the Internet, which of the following is the MOST effective means of ensuring authenticity?

A. Digital code signing
B. Digital certificates
C. Steganography
D. Digital signatures
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following is the FIRST step required to achieve effective performance measurement?
A. Define meaningful metrics.
B. Implement control objectives.
C. Select and place sensors.
D. Validate and calibrate metrics.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
After assessing risk, the decision to treat the risk should be based PRIMARILY on:
A. whether the level of risk exceeds inherent risk.
B. availability of financial resources.
C. whether the level of risk exceeds risk appetite.
D. the criticality of the risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following is the BEST way to identify the potential impact of a successful attack on an organization's mission critical applications?
A. Perform an independent code review.
B. Execute regular vulnerability scans.
C. Perform an application vulnerability review,
D. Conduct penetration testing

Answer: (SHOW ANSWER)

NEW QUESTION: 34
The PRIMARY role of an information security steering group is to ensure that:
A. security policies address business issues.
B. there is compliance with software-copyright legislation.
C. security procedures and practices are in line with formal policies.
D. there is compliance with security standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which of the following is the MOST important outcome of senior management's analysis of information security metrics?
A. The alignment of the information security budget to corporate funding
B. The alignment of security and IT objectives
C. The integration of information security with corporate governance
D. The establishment of a risk acceptance process
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which of the following is the MOST important consideration when determining the approach for gaining organization-wide acceptance of an information security plan?
A. Mature security policy
B. Organizational culture
C. Organizational information security awareness
D. Information security roles and responsibilities
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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. cost-benefit analysis.
C. risk assessment.
D. business impact analysis (BIA).
Answer: (SHOW ANSWER)

NEW QUESTION: 38
The PRIMARY benefit of integrating information security risk into enterprise risk management is to:
A. provide a holistic view of risk

B. justify the information security budget
C. obtain senior management's commitment.
D. ensure timely risk mitigation.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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: 40
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. Reviewing the business strategy
B. Performing a business impact analysis (BIA)
C. Measuring the volume of data in each system
D. Reviewing the information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following is the BEST way to facilitate the alignment between an organization's information security program and business objectives?
A. Information security is considered at the feasibility stage of all I Perform a business impact analysisT projects
B. The information security governance committee includes representation from key business areas.
C. The information security program is audited by the internal audit department
D. The chief executive officer reviews and approves the information security program.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:
A. assess the risks of all new equipment.
B. develop an approved equipment list.
C. assess security during equipment deployment.
D. ensure compliance during user acceptance testing.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
Which of the following is the FIRST task when determining an organization's information security profile?
A. Build an asset inventory.
B. Complete a threat assessment
C. Establish security standards.
D. List administrative privileges.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
An information security manager is concerned that executive management does not su the following is the BEST way to address this situation?
A. Report the risk and status of the information security program to the board.
B. Escalate noncompliance concerns to the internal audit manager
C. Demonstrate alignment of the information security function with business needs.
D. Revise the information security strategy to meet executive management expectations.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following is the BEST indication that a recently adopted information security framework is a good fit for an organization?
A. Objectives in the framework correlate directly to business practices
B. The number of security incidents has significantly declined
C. The framework includes industry-recognized information security best practices.
D. The business has obtained framework certification.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Deciding the level of protection a particular asset should be given is BEST determined by:
A. a vulnerability assessment
B. a threat assessment.
C. a risk analysis.
D. corporate risk appetite.
Answer: (SHOW ANSWER)

NEW QUESTION: 47
After an information security business case has been approved by senior management, it should be:
A. referenced to build architectural blueprints for the solution
B. reviewed at key intervals to ensure intended outcomes.
C. used to design functional requirements for the solution
D. used as the foundation for a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which of the following is the MOST effective defense against spear phishing attacks?
A. Web filtering
B. User awareness training
C. Anti-spam solution
D. Unified threat management
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which of the following is the BEST method to ensure that data owners take responsibility for implementing information security processes?
A. Provide job rotation into the security organization.
B. Include membership on project teams
C. Increase security awareness training
D. Include security tasks into employee job descriptions
Answer: (SHOW ANSWER)

NEW QUESTION: 50
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: 51

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. The data classification scheme.
B. Recovery time objectives (RTOs)
C. Key performance indicators (KPIs)
D. Recovery point objectives (RPOs)
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following metrics is MOST useful to demonstrate the effectiveness of an incident response plan?
A. Average time to respond to an incident
B. Total number of incident responses
C. Total number of reported incidents
D. Average time to resolve an incident
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which of the following would contribute MOST to employees' understanding of data handling responsibilities?
A. Labeling documents according to appropriate security classification
B. Demonstrating support by senior management of the security program
C. Implementing a tailored security awareness training program
D. Requiring staff acknowledgement of security policies
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
When trying to integrate information security across an organization, the MOST important goal for a governing body should be to ensure:
A. the resources used for information security projects are kept to a minimum.
B. information security is treated as a business critical issue.
C. periodic information security audits are conducted.
D. funding is approved for requested information security projects.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
The PRIMARY objective of periodically testing an incident response plan should be to:
A. harden the technical infrastructure.
B. improve employee awareness of the incident response process,
C. improve internal processes and procedures,

D. highlight the importance of incident response and recovery.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
The head of a department affected by a recent security incident expressed concern about not being aware of the actions taken to resolve the incident. Which of the following is the BEST way to address this issue?
A. Disseminate the incident response plan throughout the organization.
B. Discuss the definition of roles in the incident response plan.
C. Ensure better identification of incidents in the incident response plan.
D. Require management approval of the incident response plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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. Multiple KRIs for a single control process
B. Undefined thresholds to trigger alerts
C. Use of qualitative measures
D. Lack of formal KRI approval from IT management
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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. Privacy policies ire only reviewed annually
B. The organization uses a decentralized privacy governance structure
C. The organization doe* not have a dedicated privacy officer
D. The privacy program does not include a formal warning component
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Which of the following is the MOST important outcome of monitoring and reporting on information security processes?
A. Ensuring information security operations are reviewed for effectiveness
B. Ensuring information security operations support control objectives
C. Ensiling information security operations follow approved procedures
D. Ensuring information security operations meet service level agreements (SLA)
Answer: (SHOW ANSWER)

NEW QUESTION: 60

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. consult external third parties on how to treat the risk.

B. design and implement controls to reduce the risk.

C. ensure that employees are aware of the risk.

D. provide senior management with risk treatment options.

Answer: (SHOW ANSWER)

NEW QUESTION: 61

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. Identified risks and mitigating controls

B. Industry best practice benchmarking results

C. Information security-related metrics

D. Cost-benefit analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 62

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. Obtain process owner buy-in to remove the controls.

C. Perform a cost-benefit analysis on modifying the control environment

D. Perform a risk assessment on modifying the control environment.

Answer: (SHOW ANSWER)

NEW QUESTION: 63

An information security program should be established PRIMARILY on the basis of:

A. senior management input

B. the approved information security strategy.
C. the approved risk management approach.
D. data security regulatory requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
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. Perform vulnerability assessments
C. Conduct per iodic audits.
D. Conduct security awareness testing
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following provides the BEST evidence that the information security program is aligned to the business strategy?
A. Information security initiatives are directly correlated to business processes.
B. Business senior management supports the information security policies.
C. The information security program manages risk within the business1* risk tolerance.
D. The information security team is able to provide key performance indicators (KPIs) to senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following is the BEST approach to identify noncompliance issues with legal, regulatory, and contractual requirements?
A. Vulnerability assessment
B. Risk assessment
C. Gap analysis
D. Business impact analysis (B1A)
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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. Perform a root cause analysis.
B. Update the incident response plan.
C. Conduct a lessons learned exercise.
D. Implement compensating controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?
A. Implementing proactive systems monitoring
B. Updating information security awareness materials
C. Providing ongoing training to the incident response team
D. Implementing a honeypot environment
Answer: (SHOW ANSWER)

NEW QUESTION: 69
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. Results of an independent assessment
C. A report on the maturity of controls
D. Up-to-date policy and procedures documentation
Answer: (SHOW ANSWER)

NEW QUESTION: 70
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. Conduct incident response plan testing.
C. Define communication processes
D. Communicate disciplinary procedures.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Which of the following would be MOST important to consider when implementing security settings for a new system'
A. Industry best practices applicable to the business
B. Government regulations and related penalties
C. Business objectives and related IT risk
D. Results from internal and external audits
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?
A. A business case

B. Application security policy
C. Internal audit reports
D. Vulnerability assessment results
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following BEST measures the effectiveness of an organization's information security strategy?
A. Comparison of threats to vulnerabilities
B. Comparison of residual risk to risk appetite
C. Comparison of current security budget to previous year's budget
D. Comparison of mitigated risk to accepted risk
Answer: (SHOW ANSWER)

NEW QUESTION: 74
To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:
A. criteria consistent with classification levels
B. established guidelines
C. efficient technical processing considerations,
D. overall IT capacity and operational constraints,
Answer: (SHOW ANSWER)

NEW QUESTION: 75
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. Ask senior management to increase the acceptable risk levels
C. Implement more stringent countermeasures.
D. Evaluate whether an excessive level of control is being applied.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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. Business impact analysis (BIA)
B. Cost-benefit analysis
C. Risk analysis
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 77
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. Identify information security risk associated with the processes
C. Benchmark the processes with best practice to identify gaps.
D. Assess the business objectives of the processes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following would BEST help to ensure an organization s security program is aligned with business objectives?
A. Security policies are reviewed and approved by the chief information officer.
B. The organization's board of directors includes a dedicated information security specialist
C. Project managers receive annual information security awareness training.
D. The security strategy it reviewed and approved by the organization s executive committee.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
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 owner of the IT asset
B. The classification of the information processed by the IT asset
C. The replacement cost of the IT asset
D. The service level agreement (SLA) for the IT asset
Answer: (SHOW ANSWER)

NEW QUESTION: 80
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. An IT governance committee is m place.
C. Security strategy objectives are defined in business terms.
D. The security strategy is benchmarked with similar organizations
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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: 82
The PRIMARY focus of a training curriculum for members of an incident response team should be:
A. external corporate communication
B. specific role training,
C. technology training.
D. security awareness
Answer: (SHOW ANSWER)

NEW QUESTION: 83
When developing a classification method for incidents, the categories MUST be:
A. specific to situations.
B. quantitatively defined.
C. regularly reviewed.
D. assigned to incident handlers.
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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. Review and approval of IT projects by the information security manager
C. Continuous security auditing of IT service processes
D. Participation of IT stakeholders in the security program steering committee
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Information classification is a fundamental step in determining:

A. the type of metrics that should be captured
B. whether risk analysis objectives are met.
C. who has ownership of information.
D. the security strategy that should be used
Answer: (SHOW ANSWER)

NEW QUESTION: 86
An organization is considering the purchase of a competitor. To determine the competitor's security posture, the BEST course of action for the organization's information security manager would be to:
A. assess the security policy of the competitor.
B. assess the key technical controls of the competitor.
C. perform a security gap analysis on the competitor.
D. conduct a penetration test of the competitor,
Answer: (SHOW ANSWER)

NEW QUESTION: 87
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. Multi-factor login requirements for cloud service applications timeouts, and complex passwords
B. Deployment of nested firewalls within the infrastructure
C. Strict enforcement of role-based access control (RBAC)
D. Separate security controls for applications, platforms programs and endpoints
Answer: (SHOW ANSWER)

NEW QUESTION: 88
When developing an incident response plan, the information security manager should:
A. require IT to invoke the business continuity plan (BCP).
B. include response scenarios that have been approved previously by business management.
C. determine recovery time objectives (RTOs).
D. allow IT to decide which systems can be removed from the infrastructure.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:
A. maintain compliance with industry best practices.
B. serve as evidence of security awareness training.
C. maintain an accurate record of users access rights

D. assign accountability for transactions made with the user's ID.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Which of the following is the BEST reason for delaying the application of a critical security patch?
A. Lack of vulnerability management
B. Conflicts with software development life cycle
C. Technology interdependences
D. Resource limitations
Answer: (SHOW ANSWER)

NEW QUESTION: 91
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. Require management approval for policy exceptions.
B. Report violations to senior management.
C. Provide awareness training to end users.
D. Implement a mobile device management (MDM) solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
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. Defining information security requirements with internal IT
C. Requiring regular reporting from the IT service provider
D. Requiring an external security audit of the IT service provider
Answer: (SHOW ANSWER)

NEW QUESTION: 93

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: 94
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Business impact analysts
B. Continuous monitoring
C. Annual risk assessments
D. Security baselining
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
Which of the following will BEST ensure that risk is evaluated on system level changes?
A. Senior management must sign-off on changes.
B. Implement a centralized change management system.
C. Security should be integrated in the change control process.
D. System development staff receives regular security training.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
As the security program matures, which of the following reports presented to senior management provides the MOST insight on the importance of the security program7
A. The causes and impacts of security-related incidents
B. The status of approved security projects against budget
C. The contribution of security investments to business growth
D. The maturity of the security program
Answer: (SHOW ANSWER)

NEW QUESTION: 97
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. ensure that employees are aware of the risk.
B. provide senior management with risk treatment options.
C. design and implement controls to reduce the risk.
D. consult external third parties on how to treat the risk.

Answer: (SHOW ANSWER)

NEW QUESTION: 98
An organization's security was compromised by outside attackers. The organization believed that the incident was resolved. After a few days, the IT staff is still noticing unusual network traffic. Which of the following is the BEST course of action to address this situation?
A. Implement additional incident response monitoring tools.
B. Initiate the incident response process.
C. Assess the level of the residual risk.
D. Identify potential incident impact.
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which of the following BIST validates that security controls are implemented in a new business process?
A. Assess the process according to information security policy
B. Benchmark the process against industry practices
C. Verify the use of a recognized control framework
D. Review the process for conformance with information security best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 100
A risk was identified during a risk assessment. The business process owner has chosen to accept the risk because the cost of remediation is greater than the projected cost of a worst-case scenario. What should be the information security manager's NEXT course of action?

A. Determine a lower-cost approach to remediation.
B. Document and schedule a date to revisit the issue.
C. Shut down the business application.
D. Document and escalate to senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 101
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 response capability.
B. risk register.
C. current threat level.
D. risk appetite.
Answer: (SHOW ANSWER)

NEW QUESTION: 102

Which of the following is the MOST effective way to mitigate the risk of data loss in the event of a stolen laptop?
A. Utilizing a strong password
B. Deploying end-point data loss prevention software on the laptop
C. Encrypting the hard drive
D. Providing end-user awareness training focused on traveling with laptops
Answer: (SHOW ANSWER)

NEW QUESTION: 103
A new version of an information security regulation is published that requires an organization's compliance.
The information security manager should FIRST
A. perform a gap analysis against the new regulation.
B. conduct a risk assessment to determine the risk of noncompliance.
C. conduct benchmarking against similar organizations.
D. perform an audit based on the new version of the regulation
Answer: (SHOW ANSWER)

NEW QUESTION: 104
The PRIMARY purpose of a security information and event management (SIEM) system is to:
A. track ongoing incidents
B. provide status of incidents
C. identify potential incidents.
D. resolve incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following should be the MOST important consideration when implementing an information security framework?
A. Technical capabilities
B. Audit findings
C. Compliance requirements
D. Risk appetite
Answer: (SHOW ANSWER)

NEW QUESTION: 106
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. Determine the classification level of the information
B. Seek business justification from the employee

C. Block access to the cloud storage service.
D. Inform higher management of a security breach
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
Which of the following is the BEST strategy to implement an effective operational security posture?
A. Vulnerability management
B. Increased security awareness
C. Defense in depth
D. Threat management
Answer: (SHOW ANSWER)

NEW QUESTION: 108
The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the GREATEST when:
A. IDS sensors are misconfigured.
B. The IT infrastructure is diverse.
C. standard operating procedures are not formalized.
D. operations and monitoring are handled by different teams.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
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. Activate the incident response plan
C. Perform a vulnerability assessment.
D. Review audit logs from IT systems.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110

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. Vulnerability assessment

C. Risk governance framework

D. Cloud security strategy

Answer: (SHOW ANSWER)

NEW QUESTION: 111

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

A. Explain security issues associated with the solution to management.

B. Ensure a security audit is performed of the service provider.

C. Determine how to securely implement the solution.

D. Ensure the service provider has the appropriate certifications.

Answer: (SHOW ANSWER)

NEW QUESTION: 112

An information security manager has implemented an ongoing security awareness training program. Employee participation has been decreasing over the year, while the number of malware and phishing incidents from email has been increasing. What is the information security manager's BEST course of action?

A. Perform a risk assessment and share results with employees.

B. Make the training program mandatory and enforce sanctions for noncompliance.

C. Include regular phishing campaigns after each training session.

D. Report the findings to senior management with recommendations.

Answer: (SHOW ANSWER)

NEW QUESTION: 113

The BEST way to minimize errors in the response to an incident is to:

A. analyze the situation during the incident.

B. reference system administration manuals.

C. follow standard operating procedures.

D. implement vendor recommendations.

Answer: (SHOW ANSWER)

NEW QUESTION: 114

Which of the following is the- BEST method to determine whether an information security program meets an organization s business objectives?
A. Conduct an annual enterprise-wide security evaluation.
B. Perform a business impact analysis (BIA)
C. Implement performance measures.
D. Review against international security standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
An organization has decided to store production data in a cloud environment. What should be the FIRST consideration?
A. Data backup
B. Data transfer
C. Data isolation
D. Data classification
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following is the MOST important consideration when establishing an information security governance framework?
A. Security steering committee meetings are held at least monthly
B. Members of the security steering committee are trained in information security.
C. Executive management support is obtained
D. Business unit management acceptance is obtained
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which of the following metrics is the BEST indicator of an abuse of the change management process that could compromise information security?
A. High ratio of lines of code changed to total lines of code
B. Percentage of changes that include post-approval supplemental add-ons
C. Large percentage decrease in monthly change requests
D. Small number of change requests
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which of the following is MOST likely to be included in an enterprise information security policy?
A. Security monitoring strategy
B. Password composition requirements
C. Audit trail review requirements
D. Consequences of noncompliance

Answer: (SHOW ANSWER)

NEW QUESTION: 119
Which of the following is the STRONGEST indication that senior management commitment to information security is lacking within an organization?
A. Inconsistent enforcement of information security policies
B. The information security manager reports to the chief risk officer
C. A reduction in information security investment
D. A high level of information security risk acceptance
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which of the following is the responsibility of a data owner?
A. Investigating and resolving suspicious database activity
B. Maintaining the integrity of the database
C. Testing to determine whether the data can be recovered successfully
D. Classifying the data in accordance with security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 121
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. Varying employee data privacy rights
B. Translation and communication of policy
C. Differences in corporate cultures
D. Differences in mobile OS platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 122
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: 123
Which of the following would BEST help to ensure an organization's information security strategy is aligned with business objectives?
A. Establishing metrics to measure the effectiveness of the information security program
B. Requesting senior management to periodically review security incidents
C. Implementing an automated solution for monitoring information security processes
D. Establishing a change control process for continued updating of security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which of the following should be define* I FIRST when creating an organization's information security strategy?
A. Objectives
B. Policies and processes
C. Budget
D. Organizational structures
Answer: (SHOW ANSWER)

NEW QUESTION: 125
An organization's information security strategy for the coming year emphasizes reducing the risk of ransomware. Which of the following would be MOST helpful to support this strategy?
A. Perform a controls gap analysis.
B. Strengthen security controls for the IT environment.
C. Provide relevant training to all staff.
D. Create a penetration testing plan
Answer: (SHOW ANSWER)

NEW QUESTION: 126
Which of the following is MOST helpful in protecting against hacking attempts on the production network?
A. Decentralized honeypot networks
B. Security information and event management (SIEM) tools
C. Intrusion prevention systems
D. Network penetration testing
Answer: (SHOW ANSWER)

NEW QUESTION: 127
An information security manager has developed a strategy to address new information security risks resulting from recent change the business. Which of the following would be MOST important to include when presenting the strategy to senior management?
A. Results of benchmarking against industry peers
B. The impact of organizational changes on the security risk profile
C. Security controls needed for risk mitigation
D. The costs associated with business process changes
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following is the PRIMARY goal of an incident response team during a security incident?
A. Minimize disruption to business-critical operations.
B. Ensure the attackers are detected and stopped.
C. Shut down the affected systems to limit the business impact.
D. Maintain a documented chain of evidence.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Which of the following is MOST relevant for an information security manager to communicate to the board of directors?
A. Threat assessments
B. The level of exposure
C. The level of inherent risk
D. Vulnerability assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 130
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. 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's expectations.
D. Report the risk and status of the information security program to the board.
Answer: (SHOW ANSWER)

NEW QUESTION: 131
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: D (LEAVE A REPLY)

NEW QUESTION: 132
In a risk assessment after the identification of threats to organizational assets, the information security manager would:
A. request funding for the security program.
B. determine threats to be reported to upper management.
C. implement controls to achieve target risk levels.
D. evaluate the controls currently in place.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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. higher costs in supporting end users.
B. impact on network capacity.
C. lack of a device management solution.
D. decrease in end user productivity.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
The success of a computer forensic investigation depends on the concept of:
A. evidence of attack.
B. forensic chain
C. chain of attack.
D. chain of evidence.
Answer: (SHOW ANSWER)

NEW QUESTION: 135
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. Document a bong-your-own-device (BYODJ policy.
B. implement a multi-factor authentication solution.
C. Implement a mobile device management solution.
D. Require employees to sign a nondisclosure agreement
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?
A. Redundant
B. Mobile
C. Shared
D. Warm
Answer: (SHOW ANSWER)

NEW QUESTION: 137
An organization is about to purchase a rival organization. The PRIMARY reason for performing information security due diligence prior to making the purchase is to:
A. evaluate the security policy and standards.
B. determine the security exposures.
C. ensure compliance with international standards.
D. assess the ability to integrate the security department operations.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which of the following is MOST helpful to review to gain an understanding of the effectiveness of an organization s information security program?
A. Balanced scorecard
B. Cost-benefit analysis
C. Key risk indicators (KRIs)
D. External Audit results
Answer: (SHOW ANSWER)

NEW QUESTION: 139
The MOST effective way to continuously monitor an organization's cybersecurity posture is to evaluate its
A. timeliness m responding to attacks.

B. compliance with industry regulations.
C. level of support from senior management.
D. key performance indicators (KPIs).
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
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. Change control procedures
D. Incident monitoring activities
Answer: (SHOW ANSWER)

NEW QUESTION: 141
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. Systems configurations
B. Audit tights
C. Number of subscribers
D. Employee access
Answer: A (LEAVE A REPLY)

NEW QUESTION: 142
Which of the following is the MOST important reason for performing a risk analysis?
A. Promoting increased security awareness in the organization
B. Identifying and eliminating threats
C. Identifying critical information assets
D. Assigning the appropriate level of protection
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Web application firewalls are needed in addition to other intrusion prevention and detection technology PRIMARILY because:
A. they recognize web application protocols.
B. web services are prone to attacks.
C. web services require unique forensic evidence
D. they prevent modification of application source code
Answer: (SHOW ANSWER)

NEW QUESTION: 144

After undertaking a security assessment of a production system, the information security manager is MOST likely to:
A. inform the development team of any residual risks and together formulate risk reduction measures.
B. establish an overall security program that minimizes the residual risks of that production system
C. inform the IT manager of the residual risks and propose measures to reduce them.
D. inform the system owner of any residual risks and propose measures to reduce them.
Answer: (SHOW ANSWER)

NEW QUESTION: 145
The PRIMARY benefit of integrating information security activities into change management processes is to:
A. protect the organization from unauthorized changes.
B. ensure required controls are Included in changes.
C. provide greater accountability for security-related changes In the business
D. protect the business from collusion and compliance threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 146
What is the PRIMARY purpose of communicating business impact to an incident response team?
A. To provide monetary values for post-incident review
B. To provide information for communication of incidents
C. To enable effective prioritization of incidents
D. To facilitate resource allocation tor preventive measures
Answer: (SHOW ANSWER)

NEW QUESTION: 147
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. Snapshot of system logs
C. Detailed metrics
D. The incident response plan
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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. Require penetration tests before production implementation.
C. Train and test system developers m secure coding practices.
D. Conduct regular security audits during system implementation stages.
Answer: (SHOW ANSWER)

NEW QUESTION: 149
Labeling information according to its security classification:
A. enhances the likelihood of people handling information securely,
B. induces the number and type of counter measures required
C. reduces the need to identify baseline controls for each classification.
D. affects the consequences if information is handled insecurely,
Answer: (SHOW ANSWER)

NEW QUESTION: 150
An information security manager learns that a departmental system is out of compliance with the information security policy's authentication requirements. Which of the following should be the information security manager's FIRST course of action?

A. Conduct an impact analysis to quantify the associated risk
B. Request risk acceptance from senior management.
C. Submit the issue to the steering committee for escalation.
D. Isolate the noncompliant system from the rest of the network.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 151
The BEST way to ensure information security efforts and initiatives continue to support corporate strategy is by:
A. including the CIO in the information security steering committee.
B. conducting benchmarking with industry best practices.
C. including information security metrics in the organizational metrics.
D. performing periodic internal audits of the information security program
Answer: (SHOW ANSWER)

NEW QUESTION: 152
Which of the following is the BEST resource for evaluating the strengths and weaknesses of an incident response plan?
A. Documentation from preparedness tests
B. Recovery time objectives (RTOs)
C. Incident response maturity assessment
D. Mission, goals and objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 153
A PRIMARY advantage of involving business management in evaluating and managing information security risks is that they:
A. better understand the security architecture.
B. are more objective than security management,
C. can balance technical and business risks.
D. better understand organizational risks.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
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: 155
The MOST important reason to use a centralized mechanism to identify information security incidents is to:
A. prevent unauthorized changes to networks
B. detect potential fraud
C. detect threats across environments
D. comply with corporate policies
Answer: (SHOW ANSWER)

NEW QUESTION: 156
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: 157
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. Run analysis tools to detect the source of the intrusion.
B. Unplug the server from the power.
C. Restrict physical and logical access to the server.
D. Reboot the server in a secure area to search for digital evidence.
Answer: (SHOW ANSWER)

NEW QUESTION: 158
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. Building an access control matrix
B. Implementation of secure transmission protocols
C. Access through a virtual private network (VPN)
D. Request customers adhere to baseline security standards
Answer: (SHOW ANSWER)

NEW QUESTION: 159
The MOST important reason for an information security manager to be involved in a new software purchase initiative is to:
A. provide input for user requirements.
B. ensure there is software escrow in place.
C. ensure the appropriate controls are considered.
D. choose the software with the most control options.
Answer: (SHOW ANSWER)

NEW QUESTION: 160
The BEST way to encourage good security practices is to:
A. recognize appropriate security behavior by individuals
B. discipline those who fail to comply with the security policy.
C. publish the information security policy.
D. schedule periodic compliance audits.
Answer: (SHOW ANSWER)

NEW QUESTION: 161

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

NEW QUESTION: 162
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. Identify unacceptable risk levels.
C. Assess vulnerabilities.
D. Evaluate potential threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?
A. Enhanced forensic analysis
B. Improved network protection
C. Reduced need for manual analysis
D. Improved response time to incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 164
An organization's marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risk assessment. Which of the following should be the MOST important consideration?
A. The security of the third-party cloud provider
B. The information to be exchanged
C. Methods for transferring the information
D. Reputations of the external marketing companies
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Which of the following BEST helps to identify vulnerabilities introduced by changes to an organization's technical infrastructure?
A. Established security baselines

B. An intrusion detection system (IDS)
C. Penetration testing
D. Log aggregation and correlation
Answer: (SHOW ANSWER)

NEW QUESTION: 166
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. Communicate incident response procedures to staff.
C. Establish and measure key performance indicators (KPIs)
D. Obtain senior management commitment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 167
Which of the following is MOST critical for an effective information security governance framework?
A. The information security program is continually monitored.
B. Information security policies are reviewed on a regular basis.
C. Board members are committed to the information security program
D. The CIO is accountable for the information security program.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
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. Objectives in the framework correlate directly to business practices
C. The business has obtained framework certification.
D. The number of security incidents has significantly declined
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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 industry benchmarking comparisons.
B. Provide the estimated return on investment (ROI).
C. Include historical data of reported incidents.
D. Provide an analysis of current risk exposures.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
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. Perform a vendor due diligence review.
B. Determine the nature of information within the application.
C. Report the application to the IT department.
D. Notify senior management of the application.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
Which of the following should be of MOST influence to an information security manager when developing IT security policies?
A. Put and current threats
B. Compliance with regulations
C. IT security framework
D. Business strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which of the following should be reviewed to obtain a structured overview of relevant information about an information security investment?
A. Quantitative risk analysis report
B. Business case
C. Information security strategy
D. Security balanced scorecard
Answer: (SHOW ANSWER)

NEW QUESTION: 173
Which of the following provides the BEST means of ensuring business units outside of IT have their information security concerns addressed?
A. Inclusion of business unit management In the Information security steering committee
B. Targeted user security awareness programs for business units outside of IT

C. Involvement of senior management in information security policy development
D. A comprehensive list of business processes performed by each business unit
Answer: (SHOW ANSWER)

NEW QUESTION: 174
An organization has detected potential risk emerging from noncompliance with new regulations in its industry.
Which of the following is the MOST important reason to report this situation to senior management?
A. A benchmark analysis needs to be performed.
B. An external review of the risk nods to be conducted
C. Specific monitoring controls need to be implemented
D. The risk profile needs to be updated
Answer: (SHOW ANSWER)

NEW QUESTION: 175
An organization with a strict need-to-know information access policy is about to launch a knowledge management intranet. Which of the following is the MOST important activity to ensure compliance with existing security policies?
A. Ensure that access to the web site is limited to senior managers and the board.
B. Password-protect documents that contain confidential information.
C. Change organization policy to allow wider use of the new web site.
D. Develop a control procedure to check content before it is published.
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Which of the following is the GREATEST risk associated with the head of information security reporting to the chief information officer (CIO)?
A. Conflict of interest while running IT operations
B. Inadequate IT security controls to protect FT assets
C. Duplicate roles and responsibilities
D. Insufficient authority to perform duties effectively
Answer: (SHOW ANSWER)

NEW QUESTION: 177
The MAIN purpose of documenting information security guidelines for use within a large, international organization is to:
A. ensure that all business units implement identical security procedures.
B. provide evidence for auditors that security practices are adequate.
C. explain the organization's preferred practices for security.
D. ensure that all business units have the same strategic security goals.

Answer: (SHOW ANSWER)

NEW QUESTION: 178
Shortly after installation, an intrusion detection system (IDS) reports a violation. Which of the following is the MOST likely explanation?
A. A routine IDS signature file download has occurred.
B. A routine IDS log file upload has occurred,
C. The violation is a false positive.
D. An intrusion has occurred-
Answer: (SHOW ANSWER)

NEW QUESTION: 179
What should be an information security manager's FIRST step when developing a business case for a new intrusion detection system (IDS) solution?
A. Perform a cost-benefit analysis.
B. Define the issues to be addressed.
C. Conduct a feasibility study.
D. Calculate the total cost of ownership (TCO).
Answer: (SHOW ANSWER)

NEW QUESTION: 180
Which of the following should be the PRIMARY consideration for an information security manager when designing security center for a newly acquired business application?

A. The IT security architecture framework
B. Cost-benefit analysis of current controls
C. Business processes supported by the application
D. Known vulnerabilities in the application
Answer: (SHOW ANSWER)

NEW QUESTION: 181
An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is MOST important to:
A. periodically recertify access rights
B. enforce document life cycle management.
C. conduct a vulnerability assessment
D. prohibit remote access to the site.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 182
Which of the following is the MAIN concern when securing emerging technologies?
A. Compatibility with legacy systems
B. Unknown vulnerabilities
C. Applying the corporate hardening standards
D. Integrating with existing access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which of the following is the PRIMARY role of a data custodian?
A. Securing information
B. Classifying information
C. Processing information
D. Validating information
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Reviewing which of the following would provide the GREATEST Input to the asset classification process?
A. Risk assessment
B. Sensitivity of the data
C. Replacement cost of the asset
D. Compliance requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 185
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. Implement a formal process to conduct periodic compliance reviews.
B. Document and publish the responsibilities of the information security department
C. Develop an operational plan providing best practices for information security projects.

D. Develop an information security awareness campaign with senior managements support.
Answer: (SHOW ANSWER)

NEW QUESTION: 186
Which of the following has the GREATEST impact on efforts to improve an organization's security posture?
A. Supportive tone at the top regarding security
B. Regular reporting 10 senior management
C. Well-documented security policies and procedures
D. Automation of security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which of the following enables compliance with a nonrepudiation policy requirement for electronic transactions?
A. One-time passwords
B. Digital certificates
C. Digital signatures
D. Encrypted passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 188
To gain a clear understanding of the impact that a new regulatory will have on an organization's security control, an information manager should FIRST.
A. Interview senior management
B. Conduct a cost-benefit analysis
C. Perform a gap analysis
D. Conduct a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 189
An executive's personal mobile device used for business purposes is reported lost. The information security manager should respond based on:
A. mobile device configuration.
B. incident classification.
C. asset management guidelines.
D. the business impact analysis (BIA).
Answer: (SHOW ANSWER)

NEW QUESTION: 190

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 communication plan
B. An inadequate business impact analysis (BIA)
C. Lack of organization-wide security awareness
D. Lack of knowledgeable help desk staff
Answer: (SHOW ANSWER)

NEW QUESTION: 191
Which of the following BEST describes an intrusion detection system (IDS) that learns the system behaviors prior to detecting potential intrusions?
A. Anomaly-based IDS
B. Host-based IDS
C. Application-based IDS
D. Network-based IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 192
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. Solicit feedback from end users
B. Establish information security metrics.
C. Conduct quarterly penetration testing.
D. Develop timely information security risk reporting.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
In an organization implementing a data classification program, ultimate responsibility for the data on the database server lies with the:
A. information security manager.
B. business unit manager
C. database administrator
D. information technology manager.
Answer: (SHOW ANSWER)

NEW QUESTION: 194
In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?
A. Stop providing mobile devices until the organization is able to implement controls.
B. Update the corporate mobile usage policy to prohibit texting.

C. Conduct a business impact analysis (BIA) and provide the report to management
D. Include the topic of prohibited texting in security awareness training.
Answer: (SHOW ANSWER)

NEW QUESTION: 195
Which of the following defines the triggers within a business continuity plan (BCP)?
A. Disaster recovery plan
B. Information security policy
C. Gap analysis
D. Needs of the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Which of the following is MOST important to the successful implementation of an information security governance framework across the organization?
A. Organizational security controls deployed in line with regulations
B. Security management processes aligned with security objectives
C. The existing organizational security culture
D. Security policies that adhere to industry best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 197
The PRIMARY goal of a security infrastructure design is the:
A. elimination of risk exposures.
B. optimization of IT resources
C. protection of corporate assets
D. reduction of security incidents.
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Which of the following metrics would be considered an accurate measure of an information security program's performance?

A. A collection of qualitative indicators that accurately measure security exceptions
B. A single numeric score derived from various measures assigned to the security program
C. The number of key risk indicators (KRIs) identified, monitored, and acted upon
D. A combination of qualitative and quantitative trends that enable decision making
Answer: (SHOW ANSWER)

NEW QUESTION: 199
In a large organization, which of the following is the BEST source for identifying ownership of a PC?
A. Domain name server (DNS) records
B. User ID register
C. Asset management register
D. Identity management system
Answer: (SHOW ANSWER)

NEW QUESTION: 200
Which of the following is MOST important for an information security manager to ensure is included in a business case for a new security system?

A. Audit-logging capabilities
B. Benchmarking results
C. Risk reduction associated with the system
D. Effectiveness of controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?
A. Encryption
B. Report distribution
C. Retention
D. Tuning
Answer: (SHOW ANSWER)

NEW QUESTION: 202
Which of the following would BEST fulfill a board of directors' request for a concise
A. Business impact analysis
B. Balanced scorecard
C. Risk register
D. Risk heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 203
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. Scan social media sites for company-related information.
B. Train employees how to set up privacy rules on social media sites.
C. Communicate social media usage requirements and monitor compliance.
D. Block workplace access to social media sites and monitor employee usage.
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the following is MOST important for an information security manager to communicate to senior management regarding the security program?
A. User roles and responsibilities
B. Impact analysts results
C. Potential risks and exposures
D. Security architecture changes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 205
Which of the following threats is prevented by using token-based authentication?
A. Denial of service attack over the network
B. Password sniffing attack on the network
C. Session eavesdropping attack on the network
D. Man-in-the-middle attack on the client
Answer: (SHOW ANSWER)

NEW QUESTION: 206
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 periodic independent third-party reviews
B. Requiring business continuity plans (BCPs) from the vendor
C. Verifying security certifications held by the vendor
D. Reviewing the vendor's security audit reports
Answer: D (LEAVE A REPLY)

NEW QUESTION: 207
Which of the following is MOST important when selecting an information security metric?
A. Defining the metric in quantitative terms
B. Defining the metric in qualitative terms

C. Ensuring the metric is repeatable
D. Aligning the metric to the IT strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 208
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. Immediately update the information security policy to address protection of personal data
C. Seek human resources advice to make appropriate changes to the information security policy.
D. Implement information masking controls to hide personal data
Answer: (SHOW ANSWER)

NEW QUESTION: 209
A business unit has requested IT to implement simple authentication using IDs and passwords. The information security policy requires using multi-factor authentication. The information security manager should FIRST:
A. escalate the request to senior management
B. implement two-factor authentication.
C. perform a risk assessment
D. assess alignment with business objectives.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 210
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. Ability to remain current with patches
B. Generation of excessive security event logs
C. Segregation of servers from the production environment
D. Ability to maintain server security baseline
Answer: (SHOW ANSWER)

NEW QUESTION: 211
In a large organization requesting outsourced services, which of the following contract clauses is MOST important to the information security manager?
A. Frequency of status reporting
B. Nondisclosure clause
C. Intellectual property
D. Compliance with security requirements

Answer: (SHOW ANSWER)

NEW QUESTION: 212
Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?
A. Promoting security training
B. Molding periodic meetings with business owners
C. Establishing a steering committee
D. Creating communication channels
Answer: (SHOW ANSWER)

NEW QUESTION: 213
After a security incident has been contained, which of the following should be done FIRST?
A. Perform a complete wipe of the affected system.
B. Conduct forensic analysis.
C. Restore the affected system from backup.
D. Notify local authorities.
Answer: (SHOW ANSWER)

NEW QUESTION: 214
Which of the following is the GREATEST risk of single sign-on?
A. It is a single point of failure for an enterprise access control process.
B. Integration of single sign-on with the rest of the infrastructure is complicated
C. One administrator maintains the single sign-on solutions without segregation of duty.
D. Password carelessness by one user may render the entire infrastructure vulnerable
Answer: (SHOW ANSWER)

NEW QUESTION: 215
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 number of threats to an organization

C. Reduction In the cost of risk remediation for an organization
D. Reduction in the amount of risk exposure man organ nation
Answer: (SHOW ANSWER)

NEW QUESTION: 216
Which of the following is BEST determined by using technical metrics?
A. Whether controls are operating effectively.
B. How well the security strategy is aligned with organizational objectives
C. How well security risk is being managed
D. Whether security resources are adequately allocated
Answer: (SHOW ANSWER)

NEW QUESTION: 217
Which is MOST important to enable a timely response to a security breach?
A. Security event logging
B. Roles and responsibilities
C. Forensic analysis
D. Knowledge sharing and collaboration
Answer: (SHOW ANSWER)

NEW QUESTION: 218
Organization XYZ. a lucrative, Internet-only business, recently suffered a power outage that lasted 2 hours.
The organization s data center was unavailable in the interim. In order to mitigate risk in the MOST cost-efficient manner, the organization should:
A. plan to operate at a reduced capacity from the primary place of business.
B. set up a duplicate business center in a geographically separate area.
C. install an uninterruptible power supply (UPS) and generator.
D. create an FT hot site with immediate fail-over capability.
Answer: (SHOW ANSWER)

NEW QUESTION: 219
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. Comparing the recovery point objectives (RPOs)
B. Reviewing each system's key performance indicators (KPIs)
C. Evaluating the cost associated with each system's outage
D. Reviewing the business plans of each department
Answer: (SHOW ANSWER)

NEW QUESTION: 220

Which of the following is the BEST reason to separate short-term from long-term plans within an information security roadmap?

A. To allow for reactive initiatives

B. To facilitate business plan reporting to management

C. To update the roadmap according to current risks

D. To allocate resources for initiatives

Answer: (SHOW ANSWER)

NEW QUESTION: 221

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. Update the security policy

C. Design and document a new process

D. Report the issue to senior management

Answer: (SHOW ANSWER)

NEW QUESTION: 222

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. Management action plan

B. Risk register

C. Industry benchmarks

D. Trend analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 223

Utilizing external resources for highly technical information security tasks allows an information security manager to:

A. transfer business risk,

B. distribute technology risk

C. outsource responsibility,

D. leverage limited resources,

Answer: (SHOW ANSWER)

NEW QUESTION: 224

Threat and vulnerability assessments are important PRIMARILY because they are:

A. needed to estimate risk.

B. the basis for setting control objectives.
C. used to establish security investments.
D. elements of the organization's security posture.
Answer: (SHOW ANSWER)

NEW QUESTION: 225
What should be an organization'e. MAIN concern when evaluating an Infrastructure as a Service (laaS) cloud computing model for an e-commerce application?
A. Where the application resides
B. Availability of providers services
C. Internal audit requirements
D. Application ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Human resources is evaluating potential Software as a Service (SaaS) cloud services, Which of the following should the information security manager do FIRST to support..
A. Review the cloud service providers" controls reports.
B. Conduct a security audit on the cloud service providers.
C. Perform a risk assessment of adopting cloud services.
D. Perform a cost-benefit analysis of using cloud services.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 227
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 that implemented program controls are effective.
C. Demonstrate that the program enables business activities.
D. Demonstrate the readiness of business continuity plans.
Answer: (SHOW ANSWER)

NEW QUESTION: 228
Which of the following control type is the FIRST consideration for aligning employee behavior with an organization's information security objectives?
A. Physical security control
B. Technical security controls
C. Directive security
D. Logical access control
Answer: (SHOW ANSWER)

NEW QUESTION: 229
In an organization where IT is critical to its business strategy and where there is a high level of operational dependence on IT, senior management commitment to security is BEST demonstrated by the:
A. segregation of duties policy
B. reporting The of the chief information security officer (CISO)
C. size of the IT security function,
D. existence of an IT steering committee.
Answer: (SHOW ANSWER)

NEW QUESTION: 230
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. the database becomes unavailable if the password of The application ID expires.
B. an incident involving unauthorized access to data cannot be tied to a specific user
C. when multiple sessions with the same application ID collide, the database locks up
D. users can gam direct access to the application ID and circumvent data controls,
Answer: (SHOW ANSWER)

NEW QUESTION: 231
Which of the following is MOST important to include in an information security strategy?
A. Information security organizational structures and responsibilities
B. Current and future desired state of information security
C. Information security program needs
D. Cost reduction techniques for information security investments
Answer: (SHOW ANSWER)

NEW QUESTION: 232
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. Continuous monitoring of An information security risk profile
C. Evaluating the provider s security incident response plan
D. Ensuring the provider's roles and responsibilities are established
Answer: (SHOW ANSWER)

NEW QUESTION: 233
During an annual security review of an organizations servers, it was found that the customer service team's file server, which contains sensitive customer data, is accessible to all user IDs in the organization. Which of the following should the information security manager do FIRST?
A. Report The situation to the data owner.
B. Train the customer service team on properly controlling file permissions.
C. Remove access privileges to the folder containing the data.
D. Isolate the server from the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 234
Information security governance is PRIMARILY driven by which of the following?
A. Litigation potential
B. Technology constraints
C. Regulatory requirements
D. Business strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 235
A global organization has developed a strategy to share a customer information database between offices in two countries. In this situation, it is MOST important to ensure:
A. data sharing complies with local laws and regulations at both locations.
B. a nondisclosure agreement is signed.
C. risk coverage is split between the two locations sharing data.
D. data is encrypted in transit and at rest
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which of the following would BEST mitigate identified vulnerabilities in a timely manner?
A. Continuous vulnerability monitoring tool
B. Action plan with responsibilities and deadlines
C. Monitoring of key risk indicators (KRIs)
D. Categorization of the vulnerabilities based on system's criticality
Answer: (SHOW ANSWER)

NEW QUESTION: 237

A threat intelligence report indicates there has been a significant rise in the number of attacks targeting the industry. What should the information security manager do NEXT?

A. Allocate additional resources to monitor perimeter security systems,

B. Conduct penetration testing to identity vulnerabilities.

C. Update the organization's security awareness campaign.

D. Discuss the risk with senior management.

Answer: (SHOW ANSWER)

NEW QUESTION: 238

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

A. the importance of the function to be tested and the cost of testing,

B. the experience level of personnel and the function location.

C. manual processing capabilities and the test location

D. prior testing results and the degree of detail of the business continuity plan

Answer: (SHOW ANSWER)

NEW QUESTION: 239

An organization establishes an internal document collaboration site. To ensure data confidently of each project group, it is MOST important to:

A. Conduct vulnerability assessment

B. Periodically recertify access rights.

C. Prohibit remote access to the site

D. Enforce document life cycle management

Answer: (SHOW ANSWER)

NEW QUESTION: 240

Which of the following will BEST enable an effective information asset classification process?

A. Assigning ownership

B. Reviewing the recovery time objective (RTO) requirements of the asset

C. Analyzing audit findings

D. Including security requirements in the classification process

Answer: (SHOW ANSWER)

NEW QUESTION: 241

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

A. Encourage staff to report any suspicious activities.

B. Provide incident management training to all start.

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

D. Implement an acceptable use policy.

Answer: (SHOW ANSWER)

NEW QUESTION: 242
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. is hosted by a cloud service provider
D. has not been updated with the latest patches
Answer: (SHOW ANSWER)

NEW QUESTION: 243
An organization is considering a self-service solution for the deployment of virtualized development servers.
A. Generation of excessive security event logs
B. Segregation of servers from the production environment
C. Ability to remain current with patches
D. Ability to maintain server security baseline
Answer: (SHOW ANSWER)

NEW QUESTION: 244
Relying on which of the following methods when detecting new threats using IDS should be of MOST concern?
A. Attack signatures
B. Traffic analysis
C. Statistical pattern recognition
D. Heuristic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 245
When introducing security measures into a software development life cycle, which of the following should be the FIRST step?
A. Conduct static code analysis.

B. Institute a peer review
C. Perform benchmarking.
D. Create a threat model.
Answer: (SHOW ANSWER)

NEW QUESTION: 246
Which of the following is the MOST significant benefit of effective change management?
A. All provisioned modifications are approved by information security.
B. Information security management is Involved with the change advisory board.
C. Release management is considered in the process.
D. Security implications are considered as a standard practice.
Answer: (SHOW ANSWER)

NEW QUESTION: 247
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. Structured walk-through
B. Simulation testing
C. Checklist review
D. Parallel testing
Answer: (SHOW ANSWER)

NEW QUESTION: 248
It is MOST important tot an information security manager to ensure that security risk assessments are performed:
A. during a root cause analysis
B. as part of the security business case
C. In response to the threat landscape,
D. consistently throughout the enterprise.
Answer: (SHOW ANSWER)

NEW QUESTION: 249
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. Penetration testing of network devices
C. Endpoint baseline configuration analysis
D. Vulnerability assessment of network devices
Answer: (SHOW ANSWER)

NEW QUESTION: 250

Which of the following BEST demonstrates effective information security management within an organization?

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

NEW QUESTION: 251
To integrate security into system development fie cycle (SDLC) processes, an organization MUST ensure that security.
A. Roles and responsibly have been defined
B. Is a represented on the configuration control board.
C. Performance metrics have been met.
D. Is a prerequisite for complete of major phases
Answer: (SHOW ANSWER)

NEW QUESTION: 252
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 risk assessment
B. Results of a red team exercise
C. Results of a security pokey review
D. Results of a vulnerability scan
Answer: (SHOW ANSWER)

NEW QUESTION: 253
Failure to include information security requirements within the build/buy decision would MOST likely result in the need for:
A. security scanning of operational platforms
B. compensating controls in the operational environment.
C. more stringent source programming standards.
D. commercial product compliance with corporate standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 254
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: 255
Which of the following is MOST important to building an effective information security program?
A. Relevant and timely content included in awareness programs
B. Management support for information security
C. logical access controls for information systems
D. Information security architecture to increase monitoring activities
Answer: (SHOW ANSWER)