ISACA.CISM.v2021-02-08.q399

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	399
Version:	v2021-02-08
# of views:	114
# of Questions views:	3990

https://www.freecram.com/torrent/ISACA.CISM.v2021-02-08.q399.html

NEW QUESTION: 1
Web application firewalls are needed in addition to other intrusion prevention and detection technology PRIMARILY because:
A. they recognize web application protocols.
B. they prevent modification of application source code
C. web services are prone to attacks.
D. web services require unique forensic evidence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following is MOST important when carrying out a forensic examination of a laptop to determine an employee s involvement in a fraud?
A. The employee's network access should be suspended.
B. The laptop should not be removed from the company premises.
C. An HR representative should be present during the laptop examination.
D. The investigation should be conducted on an image of the original disk drive.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
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 the business plans of each department
C. Evaluating the cost associated with each system's outage
D. Reviewing each system's key performance indicators (KPIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 4

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

NEW QUESTION: 5
Which of the following would BEST mitigate identified vulnerabilities in a timely manner?
A. Action plan with responsibilities and deadlines
B. Categorization of the vulnerabilities based on system's criticality
C. Monitoring of key risk indicators (KRIs)
D. Continuous vulnerability monitoring tool
Answer: (SHOW ANSWER)

NEW QUESTION: 6
In a large organization requesting outsourced services, which of the following contract clauses is MOST important to the information security manager?
A. Intellectual property
B. Compliance with security requirements
C. Frequency of status reporting
D. Nondisclosure clause
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
An organization has decided to migrate a customer facing on-premise application to a cloud provider. Which of the following would be MOST helpful when assessing the proposed data backup requirements prior to the migration?
A. Risk assessment
B. Control assessment
C. Business impact analysis (BIA)
D. Vendor controls report analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
An organization has established information security policies, but the information security the MOST likely reason for this situation?
A. The information security policies lack alignment with corporate goals.
B. The organization is operating in a highly regulated industry.
C. The information security program is not adequately funded.

D. The information security policies are not communicated across the organization.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
An information security manager is reviewing the organization's incident response policy affected by a proposed public cloud integration. Which of the following will be the MOST difficult to resolve with the cloud service provider?
A. Accessing information security event data
B. Regular testing of incident response plan
C. Obtaining physical hardware for forensic analysis
D. Defining incidents and notification criteria
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
A risk has been formally accepted and documented. Which of the following is the MOST important action for an information security manager?
A. Re-evaluate the organization's risk appetite
B. Update risk tolerance levels.
C. Notify senior management and the board.
D. Monitor the environment for changes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
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. Coordinating IRT
B. Holistic IRT
C. Central IRT
D. Distributed IRT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?
A. Identifying risk mitigation options
B. Identifying critical business processes
C. Identifying the threat environment
D. Identifying key business risks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
An information security manager is implementing a bring your own device (BYOD) program. Which of the following would BEST ensure that users adhere to the security standards?
A. Deploy a device management solution.
B. Publish the standards on the intranet landing page.
C. Monitor user activities on the network.
D. Establish an acceptable use policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
In a large organization, defining recovery time objectives (RTOs) is PRIMARILY the responsibility of;
A. senior management
B. the business unit manager.
C. the IT manager
D. the information security manager.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
The effectiveness of an information security governance framework will BEST be enhanced if:
A. risk management is built into operational and strategic activities.
B. IS auditors are empowered to evaluate governance activities,
C. a culture of legal and regulatory compliance is promoted by management.
D. consultants review the information security governance framework
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Which of the following is the PRIMARY purpose of data classification?
A. To select encryption technology
B. To determine access rights to data
C. To ensure integrity of data
D. To provide a basis for protecting data
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following is the MOST effective method for categorizing system and data criticality during the risk assessment process?
A. Interview the asset owners.
B. Interview data custodians.
C. Interview members of the board.
D. Interview senior management.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
An IT department plans to migrate an application to the public cloud. Which of the following is the information security manager's MOST important action in support of this initiative?
A. Provide cloud security requirements.
B. Evaluate service level agreements (SLAs).
C. Calculate security implementation costs.
D. Review cloud provider independent assessment reports.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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: 20
Which of the following is the PRIMARY benefit of implementing a maturity model for information security management?
A. Information security strategy will be in line with industry best practice
B. Staff awareness of information security compliance will be promoted.
C. Gaps between current and desirable levels will be addressed.
D. Information security management costs will be optimized.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
An information security manager wants to implement a security Information and event management (SIEM) system that will aggregate log data from all systems that control perimeter access. Which of the following would BEST support the business case for this initiative to senior management?
A. Independent evidence of SIEM system's ability to reduce risk
B. Metrics related to the number of systems to be consolidated
C. Alignment with industry best practices
D. Industry examples of threats detected using a SIEM system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
Which of the following is the MOST effective way for an Information security manager to ensure that security is incorporated into an organization's project development processes?
A. Participate in project initiation, approval, and funding.
B. Conduct security reviews during design, testing and implementation
C. Develop good communications with the project management office
D. Integrate organization's security requirements into project management.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
An organization has experienced a ransomware attack. Which of the following is the BEST course of action to prevent further attacks?
A. Update the security policy.
B. Implement application whitelisting.
C. Refuse to pay the ransom.
D. Implement application blacklisting.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
Risk identification, analysis, and mitigation activities can BCST be integrated into business life cycle processes by linking them to:
A. continuity planning
B. configuration management.
C. change management
D. compliance testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
When developing security standards, which of the following would be MOST appropriate to include?

A. Acceptable use of IT assets
B. Accountability for licenses
C. Inventory management
D. Operating system requirements
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following is the BEST indicator to demonstrate whether information security investments are optimally supporting organizational objecti.....
A. Percentage of security-related initiatives completed within budget
B. Ratio of security costs to the value of assets
C. Percentage of current security resource utilization
D. Ratio of security incidents from known risk versus unidentified risk
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which of the following is the BEST way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)*?
A. Establish and present appropriate metrics that track performance
B. Perform industry research annually and document the overall ranking of the IPS
C. Perform a penetration test to demonstrate the ability to protect
D. Provide yearly competitive pricing to illustrate the value of the IPS.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following is the PRIMARY purpose for establishing a bring your own device (BYOD) policy that only permits application downloads from designated online markets.
A. Protect against malware-based attacks.
B. Allow IT to monitor application usage.
C. Enhance IT application support for users.
D. Conserve storage for approved applications.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following would be the MOST important information to include in a business case for an information security project in a highly regulated industry?
A. Compliance risk assessment
B. Number of reported security incidents
C. Industry comparison analysis
D. Critical audit findings
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
When designing security controls, it is MOST important to:
A. focus on preventive controls.
B. evaluate the costs associated with the controls.
C. apply a risk-based approach.
D. apply controls to confidential information.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following should be communicated FIRST to senior management once an information security incident has been contained?
A. The initial business impact of the incident
B. Whether the recovery time objective was met
C. Details on containment activities
D. A summary of key lessons learned from the incident
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
What is the MOST important role of an organization's data custodian in support of the information security function?
A. Evaluating data security technology vendors
B. Approving access rights to departmental data
C. Assessing data security risks to the organization
D. Applying approved security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 33
In an organization implementing a data classification program, ultimate responsibility for the data on the database server lies with the:
A. information technology manager.
B. business unit manager

C. information security manager.
D. database administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which of the following is the MOST effective approach to ensure IT processes are performed in compliance with the information security policies?
A. Allocating sufficient resources
B. Ensuring that key controls are embedded in the processes
C. Providing information security policy training to the process owners
D. Identifying risks in the processes and managing those risks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
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. Develop an operational plan providing best practices for information security projects.
B. Develop an information security awareness campaign with senior managements support.
C. Implement a formal process to conduct periodic compliance reviews.
D. Document and publish the responsibilities of the information security department
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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. Determine the nature of information within the application.
B. Perform a vendor due diligence review.
C. Notify senior management of the application.
D. Report the application to the IT department.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following BEST enables effective closure of noncompliance issues?
A. Insuring against the risk
B. Performing control self-assessments (CSAs)
C. Capturing issues in a risk register
D. Executing an approved mitigation plan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 38
What should an information security manager do FIRST upon learning that the third-party provider responsible for a mission-critical process is subcontracting critical functions to other providers?
A. Request a formal explanation from the third party.
B. Review the provider's contract
C. Adjust the insurance policy coverage.
D. Engage an external audit of the third party.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
What should be an information security manager's PRIMARY objective in the event of a security incident?
A. Identify lapses in operational control effectiveness.
B. Identify the source of the breach and how it was perpetrated.
C. Ensure that normal operations are not disrupted.
D. Contain the threat and restore operations in a timely manner.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organizations information security manager?
A. Documentation of the change was made after implementation.
B. The information security manager did not review the change prior to implementation.
C. The change did not include a proper assessment of risk.
D. The operations team implemented the change without regression testing,
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
Which of the following is MOST effective against system intrusions?
A. Two-factor authentication
B. Continuous monitoring
C. Layered protection
D. Penetration testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
Which of the following metrics provides the BEST indication of the effectiveness of a security awareness campaign?

A. User approval rating of security awareness classes
B. Quiz scores for users who took security awareness classes
C. Percentage of users who have taken the courses
D. The number of reported security events
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
An information security program should be established PRIMARILY on the basis of:
A. data security regulatory requirements.
B. the approved information security strategy.
C. senior management input
D. the approved risk management approach.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
The BEST way to minimize errors in the response to an incident is to:
A. reference system administration manuals.
B. analyze the situation during the incident.
C. follow standard operating procedures.
D. implement vendor recommendations.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following is BEST to include in a business case when the return on investment (RIO) for an information security initiative is difficult to calculate?
A. Projected costs over time
B. Estimated reduction in risk
C. Projected increase in maturity level
D. Estimated increase in efficiency
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
In information security governance, the PRIMARY role of the board of directors is to ensure:
A. alignment with the strategic goals of the organization
B. compliance with regulations and best practices
C. communication of security posture to stakeholders.
D. approval of relevant policies and standards.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 47
Senior management has allocated funding to each of the organization s divisions to address information security vulnerabilities The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?
A. Redundant controls may be implemented across divisions.
B. Information security governance could be decentralized by division.
C. Return on investment may be inconsistently reported to senior management
D. Areas of highest risk may not be adequately prioritized for treatment.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
An attacker was able to gain access to an organizations perimeter firewall and made changes to allow wider external access and to steal dat a. Which of the following would have BEST provided timely identification of this incident?
A. Deploying a security information and event management system (SIEM)
B. Conducting regular system administrator awareness training
C. Implementing a data loss prevention (DLP) suite
D. Deploying an intrusion prevention system (IPS)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
An online trading company discovers that a network attack has penetrated the firewall What should be the information security manager's FIRST response?
A. Examine firewall logs to identity the attacker
B. Notify the regulatory agency of the incident
C. Evaluate the impact to the business.
D. Implement mitigating controls
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which of the following should be of MOST influence to an information security manager when developing IT security policies?

A. Compliance with regulations
B. Put and current threats
C. Business strategy
D. IT security framework
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
An information security manager finds that corporate information has been stored on a public cloud storage site for business collaboration purposes. Which of the following should be the manager's FIRST action?
A. Implement a data encryption strategy.
B. Determine the risk to the data.
C. Assign a data classification label.
D. Update service level agreements (SLAs).
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
A security team is conducting its annual disaster recovery test. Post-restoration testing shows the system response time is significantly slower due to insufficient bandwidth for Internet connectivity at the recovery center. Which of the following is the security manager's BEST course of action?
A. Halt the test until the network bandwidth is increased.
B. Document the deficiency for review by business leadership.
C. Pursue risk acceptance for the slower response time
D. Reduce the number of applications marked as critical.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
The PRIMARY purpose of a security information and event management (SIEM) system is to:
A. identify potential incidents.
B. provide status of incidents
C. resolve incidents
D. track ongoing incidents
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following is an information security manager's MOST important consideration during the investigative process of analyzing the hard drive of 3 compromises..
A. Notifying the relevant stakeholders
B. Determining the classification of stored data

C. Identifying the relevant strain of malware
D. Maintaining chain of custody
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following would provide senior management with the BEST information to better understand the organization's information security risk profile?
A. Scenarios that have a monetary impact
B. Scenarios that impact business operations
C. Scenarios that disrupt client services
D. Scenarios that impact business goals
Answer: D (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?
A. Capability to take a snapshot of virtual machines
B. Capability of online virtual machine analysis
C. Availability of web application firewall logs
D. Availability of current infrastructure documentation
Answer: (SHOW ANSWER)

NEW QUESTION: 57
The PRIMARY disadvantage of using a cold-site recovery facility is that it is:
A. only available if not being used by the primary tenant,
B. not possible to reserve test dates m advance
C. unavailable for testing during normal business hours.
D. not cost-effective for testing critical applications at the site
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which is MOST important to enable a timely response to a security breach?
A. Roles and responsibilities
B. Forensic analysis
C. Knowledge sharing and collaboration
D. Security event logging
Answer: (SHOW ANSWER)

NEW QUESTION: 59

Which of the following should be of GREATEST concern to a newly hired information security manager regarding security compliance?
A. Lack of security audits
B. Lack of standard operating procedures
C. Lack of risk assessments
D. Lack of executive support
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
What is the BEST way for a customer to authenticate an e-commerce vendor?
A. Encrypt the order using the vendor s private key
B. Use a secure communications protocol for the connection.
C. Verify the vendor's certificate with a certificate authority.
D. Request email verification of the order
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
Information classification is a fundamental step in determining:
A. who has ownership of information.
B. the security strategy that should be used
C. the type of metrics that should be captured
D. whether risk analysis objectives are met.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which of the following is the BEST indicator that an organization is appropriately managing risk?
A. The number of security incident events reported by staff has increased
B. The number of events reported from the intrusion detection system (IDS) has declined.
C. A penetration test does not identify any high-risk system vulnerabilities
D. Risk assessment results are within tolerance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
A large organization is considering a policy that would allow employees to briog their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:
A. impact on network capacity.
B. higher costs in supporting end users.
C. decrease in end user productivity.
D. lack of a device management solution.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
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. implement a multi-factor authentication solution.
B. Require employees to sign a nondisclosure agreement
C. Implement a mobile device management solution.
D. Document a bong-your-own-device (BYOD) policy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following is the MOST relevant source of information for determining the available internal human resources for executing the information security program?
A. Skills inventory
B. Roles and responsibilities matrix
C. RACI chart
D. Job descriptions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?
A. Penetration resting
B. Business
C. Risk assessment
D. Gap analysis
E. impact analysis (BIA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 67

An internal control audit has revealed a control deficiency related to a legacy system where the compensating controls no longer appear to be effective. Which of the following would BEST help the information security manager determine the security requirements to resolve the control deficiency?
A. Cost-benefit analysis
B. Risk assessment
C. Gap analysis
D. Business case
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
Which of the following BEST indicates senior management support for an information security program?
A. Detailed information security policies are established and regularly reviewed.
B. Key performance indicators (KPIs) are defined for the information security program.
C. Risk assessments are conducted frequently by the information security team.
D. The information security manager meets regularly with the lines of business.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
Which of the following is the MOST effective approach of delivering security incident response training?
A. Perform role-playing exercises to simulate real-world incident response scenarios.
B. Include incident response training within new staff orientation.
C. Engage external consultants to present real-world examples within the industry.
D. Provide on-the-job training and mentoring for the incident response team.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
Which of the following should be the PRIMARY input when defining the desired state of security within an organization?
A. Level of business impact
B. Annual loss expectancy
C. Acceptable risk level
D. External audit results
Answer: A (LEAVE A REPLY)

NEW QUESTION: 71
A new program has been implemented to standardize security configurations across a multinational organization Following implementation, the configuration standards should:
A. be changed for different subsets of the systems to minimize impact,

B. be updated to address emerging threats and vulnerabilities.
C. not deviate from industry best practice baselines.
D. remain unchanged to avoid variations across the organization
Answer: B (LEAVE A REPLY)

NEW QUESTION: 72
The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:
A. assessed level of security risk at a particular point m time.
B. level of compliance with internal policy.
C. security program priorities to achieve an accepted risk level.
D. current and target security state for the business.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
Senior management commitment and support will MOST likely be offered when the value of information security governance is presented from a:
A. compliance perspective
B. risk perspective.
C. policy perspective.
D. threat perspective.
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following would BEST enable effective decision-making?
A. A consistent process to analyze new and historical information risk
B. Annualized loss estimates determined from past security events
C. A universally applied list of generic threats, impacts, and vulnerabilities
D. Formalized acceptance of risk analysis by business management
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following would BEST enable management to be aware of an electronic breach to an externally hosted database?
A. Obligate the vendor to report suspicious activity and database breaches.
B. Implement tog monitoring of the database environment for suspicious activity.
C. Review independent audit reports of the vendors data center environment.
D. Implement a dedicated firewall configured to block suspicious activity.
Answer: (SHOW ANSWER)

NEW QUESTION: 76

An organization establishes an internal document collaboration site. To ensure data confidently of each project group, it is MOST important to:
A. Enforce document life cycle management
B. Prohibit remote access to the site
C. Conduct vulnerability assessment
D. Periodically recertify access rights.
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS) attack on a publicly facing .....
A. Defacement of website content
B. Unauthorized access to resources
C. Execution of unauthorized commands
D. Prevention of authorized access
Answer: (SHOW ANSWER)

NEW QUESTION: 78
The MOST likely cause of a security information event monitoring (SIEM) solution failing to identify a serious incident is that the system:
A. has not been updated with the latest patches
B. has performance issues
C. is not collecting logs from relevant devices.
D. is hosted by a cloud service provider
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Labeling information according to its security classification:
A. affects the consequences if information is handled insecurely,
B. reduces the need to identify baseline controls for each classification.
C. induces the number and type of counter measures required
D. enhances the likelihood of people handling information securely,

Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
An organization us& a particular encryption protocol for externally facing web pages and key financial services. A security firm publicizes a critical security flaw in the encryp manager do FIRST?
A. Activate the incident response team.
B. Remediate the vulnerability.
C. Perform a risk assessment.
D. Isolate potentially vulnerable systems.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
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: D (LEAVE A REPLY)

NEW QUESTION: 82
Which of the following is MOST helpful in determining the prioritization of available incident response resources?
A. Training of the incident response team
B. Defined incident escalation processes
C. Security metrics based on previous incidents
D. Adequate funding allocation
Answer: (SHOW ANSWER)

NEW QUESTION: 83
An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?
A. Assess the consequences of noncompliance,
B. Document risk acceptances.
C. Revise the organization s security policy
D. Conduct an information security audit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84

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

NEW QUESTION: 85
Which of the following is the GREATEST benefit of a centralized approach to coordinating information security?
A. Integration with business functions
B. Optimal use of security resources
C. Reduction in the number of policies
D. Business user buy-in
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
Which of the following is the GREATEST benefit of integrating information security program requirements into vendor management?
A. The ability to define service level agreements (SLAs)
B. The ability to improve vendor performance
C. The ability to reduce risk in the supply chain
D. The ability to meet industry compliance requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following is the PRIMARY reason to invoke continuity and recovery plans?
A. To protect corporate networks
B. To coordinate with senior management
C. To achieve service delivery objectives
D. To enforce service level agreements (SLAs)
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following BEST enables an effective escalation process within an incident response program?
A. Defined incident thresholds
B. Dedicated funding for incident management
C. Monitored program metrics
D. Adequate incident response staffing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
Which of the following will BEST enable the identification of appropriate controls to prevent repeated occurrences of similar types of information.....
A. Perform a business impact analysis (BIA) of the security incidents.
B. Review lessons learned with key stakeholders.
C. Review existing preventive controls for security weaknesses.
D. Perform a root cause analysis of the security incidents.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
Penetration testing is MOST appropriate when a:
A. new system is being designed.
B. security policy is being developed
C. new system is about to go live.
D. security incident has occurred.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
When training an incident response team, the advantage of using tabletop exercises is that they:
A. remove the need to involve senior managers in the response process.
B. provide the team with practical experience in responding to incidents.
C. ensure that the team can respond to any incident
D. enable the team to develop effective response interactions.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Which of the following is the BEST way for an Information security manager to gain wider acceptance for an information security policy that is perceived as restrictive?
A. Communicate the policy across the organization using various media.

B. Remove the restrictive requirements from the policy.
C. Review the policy with the information security steering committee.
D. Establish sanctions for failure to follow the policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
After a server has been attacked, which of the following is the BEST course of action?
A. Review vulnerability assessment
B. Isolate the system.
C. Conduct a security audit
D. Initiate modem response
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Which of the following would provide the BEST input to a business case for a technical solution to address potential system vulnerabilities?
A. Risk assessment
B. Penetration test results
C. Business impact analysis (BIA)
D. Vulnerability scan results
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following is MOST important when selecting a third-party security operations center?
A. Business continuity plans
B. Indemnity clauses
C. Independent controls assessment
D. Incident response plans
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
Which of the following is MOST critical for an effective information security governance framework?
A. Information security policies are reviewed on a regular basis.
B. The CIO is accountable for the information security program.
C. The information security program is continually monitored.
D. Board members are committed to the information security program
Answer: (SHOW ANSWER)

NEW QUESTION: 97

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. Classifying the data in accordance with security policy
D. Testing to determine whether the data can be recovered successfully
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
Which of the following BEST supports the alignment of information security with business functions?
A. A focus on technology security risk within business processes
B. Creation of a security steering committee
C. Business management participation in security penetration tests
D. IT management support of security assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 99
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: D (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following roles should be separated?
A. Help desk and security administration
B. Firewall management and security operations
C. Systems analysis and application programming
D. Data security and database administration
Answer: (SHOW ANSWER)

NEW QUESTION: 101
System logs and audit logs for sensitive systems should be stored
A. on a shared Internal server
B. on a cold site server.
C. In an encrypted folder on each server.
D. on a dedicated encrypted storage server,
Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
An organization was forced to pay a ransom to regain access to a critical database that had been encrypted in a ransomware attack. What would have BEST prevented The need to make this ransom payment?
A. Storing backups on a segregated network.
B. Training employees on ransomware
C. Verifying the firewall is configured properly
D. Ensuring all changes are approved
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
What should be an organization'.MAIN concern when evaluating an Infrastructure as a Service (IaaS) cloud computing model for an e-commerce application?
A. Application ownership
B. Availability of providers services
C. Internal audit requirements
D. Where the application resides
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
Which of the following is the MOST important consideration when determining the approach for gaining organization-wide acceptance of an information security plan?
A. Organizational information security awareness
B. Information security roles and responsibilities
C. Organizational culture
D. Mature security policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
Which of the following is the PRIMARY objective of reporting security metrics to stakeholders?
A. To demonstrate alignment to the business strategy
B. To provide support for security audit activities
C. To identify key controls within the organization
D. To communicate the effectiveness of the security program
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
Which of the following is the MOST important reason to develop an organizational threat profile?
A. To implement a proactive approach for threat management

B. To support business cases for information security investments
C. To develop threat briefings for senior management
D. To support risk treatment decisions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
Which of the following is MOST helpful in integrating information security governance with corporate governance?
A. Providing independent reports of information security efficiency and effectiveness to the board
B. Including information security processes within operational and management processes
C. Aligning the information security governance to a globally accepted framework
D. Assigning the implementation of information security governance to the steering committee
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
Which of the following should be the PRIMARY consideration when developing a security governance framework for an enterprise?
A. Assessment of the current security architecture
B. Results of a business impact analysis (BIA)
C. Benchmarking against industry best practice
D. Understanding of the current business strategy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
An organization s senior management wants to allow employees to access an internal application using their personal mobile devices. Which of the following should be the information security managers FIRST course of action?
A. Assess the security risk
B. Conduct security testing
C. Require device encryption

D. Develop a personal device policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following provides the BEST input to maintain an effective asset classification program?
A. Risk heat map
B. Vulnerability assessment
C. Annual toss expectancy
D. Business impact analysis (BIA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
Which of the following is the MOST important reason for performing a cost-benefit analysis when implementing a security control?
A. To present a realistic information security budget
B. To justify information security program activities
C. To ensure that benefits are aligned with business strategies
D. To ensure that the mitigation effort does not exceed the asset value
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
Which of the following will BEST enable an effective information asset classification process?
A. Analyzing audit findings
B. Including security requirements in the classification process
C. Reviewing the recovery time objective (RTO) requirements of the asset
D. Assigning ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Which of the following approaches is BEST for selecting controls to minimize information security risks?
A. Cost-benefit analysis
B. Risk assessment
C. Control-effectiveness evaluation
D. Industry best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 114

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

NEW QUESTION: 115
Which of the following is an information security manager's BEST course of action upon learning of new cybersecurity regulatory requirements that apply to the organization?
A. Implement the new requirements immediately.
B. Treat the new requirements as an operational issue.
C. Perform a gap analysis of the new requirements.
D. Escalate the issue to senior management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following provides the GREATEST assurance that information security is addressed in change management?
A. Requiring senior management sign-off on change management
B. Providing security training for change advisory board
C. Performing a security audit on changes
D. Reviewing changes from a security perspective
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:
A. information security management understands business performance issues.
B. the security policy is changed to accommodate IT performance pressure.
C. noncompliance issues are reported to senior management.
D. senior management provides guidance and dispute resolution.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which of the following threats is prevented by using token-based authentication?
A. Password sniffing attack on the network
B. Denial of service attack over the network
C. Session eavesdropping attack on the network
D. Man-in-the-middle attack on the client

Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
A business unit uses e-commerce with a strong password policy. Many customers complain that they cannot remember their password because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST.
A. Change the password policy to improve the customer experience
B. Recommended implementing two-factor authentication.
C. Evaluate the impact of the customer's experience on business revenue.
D. Reach alternative secure of identify verification
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
Which of the following presents the GREATEST information security concern when deploying an identity and access management solution?
A. Gaining end user acceptance
B. Supporting multiple user repositories
C. Supporting legacy applications
D. Complying with the human resource policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
Which of the following measures BEST indicates an improvement in the information security program to stakeholders?
A. A reduction in reported viruses
B. A decrease in click rates during phishing simulations
C. An increase in awareness training quiz pass rates
D. A downward trend in reported security incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 122

Which of the following is MOST important to consider when defining control objectives?
A. The organization's strategic objectives
B. The current level of residual risk
C. The organization's risk appetite
D. Control recommendations from a recent audit
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following is the BEST method to ensure that data owners take responsibility for implementing information security processes?
A. Include membership on project teams
B. Provide job rotation into the security organization.
C. Increase security awareness training
D. Include security tasks into employee job descriptions
Answer: (SHOW ANSWER)

NEW QUESTION: 124
An organization has concerns regarding a potential advanced persistent threat (APT). To ensure that the risk associated with this threat is appropriately managed, what should be the organization 5 FIRST action?
A. Implement additional controls.
B. Report to senior management.
C. Initiate incident response processes.
D. Conduct an impact analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 125
An organization is the victim of an attack generating multiple incident reports. Which of the following will BEST enable incident handling and contain exposure?
A. The ability to isolate and secure the affected systems
B. The ability to sort and classify events
C. The ability to effectively escalate incidents
D. The ability to acquire the appropriate resources
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?
A. Security supports and protects the business.
B. Effective security eliminates risk to the business.
C. Adopt a recognized framework with metrics.

D. Security is a business product and not a process.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
A business previously accepted the risk associated with a zero-day vulnerability The same vulnerability was recently exploited in a high-profile attack on another organization m the same Industry Which of the following should be the information security manager's FIRST course of action?
A. Develop best and worst case scenarios
B. Report the breach of the other organization to senior management
C. Evaluate the cost of remediating the vulnerability
D. Reassess the risk in terms of likelihood and impact
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
When supporting a large corporation's board of directors in the development of governance, which of the following is the PRIMARY function of the information security manager?
A. Developing a balanced scorecard
B. Preparing the security budget
C. Gaining commitment of senior management
D. Providing advice and guidance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
What should be the information security manager s MOST important consideration when planning a disaster recovery test?
A. Stakeholder notification procedures
B. Impact to production systems
C. Organization-wide involvement
D. Documented escalation processes
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Authorization can BEST be accomplished by establishing:
A. whether users are who they say they are
B. how users identify themselves to information systems.
C. who users can do when they are granted system access.
D. the ownership of the data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
BEST way to isolate corporate data stored on employee-owned mobile devices would be to implement:
A. a sandbox environment
B. a strong password policy
C. two-factor authentication
D. device encryption,
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
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: D (LEAVE A REPLY)

NEW QUESTION: 133
Which of the following is the BEST way for an information security manager to identify compliance with information security policies within an organization?
A. Perform vulnerability assessments
B. Conduct security awareness testing
C. Conduct per iodic audits.
D. Analyze system logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
Which of the following is the MOST significant security risk in IT asset management?
A. IT assets may be used by staff for private purposes.
B. Unregistered IT assets may not be configured properly.
C. Unregistered IT assets may riot be included in security documentation.
D. Unregistered IT assets may not be supported.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 135
Which of the following would provide the BEST justification for a new information security investment?
A. Projected reduction in risk
B. Defined key performance indicators (KPIs)
C. Results of a comprehensive threat analysis

D. Senior management involvement in project prioritization
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following is the BEST reason to separate short-term from long-term plans within an information security roadmap?
A. To update the roadmap according to current risks
B. To allow for reactive initiatives
C. To allocate resources for initiatives
D. To facilitate business plan reporting to management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 137
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Annual risk assessments
B. Security baselining
C. Continuous monitoring
D. Business impact analysts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Which of the following is MOST likely to drive an update to the information security strategy?
A. A recent penetration test has uncovered a control weakness.
B. A new chief technology officer has been hired
C. Management has decided to implement an emerging technology.
D. A major business application has been upgraded.
Answer: (SHOW ANSWER)

NEW QUESTION: 139

Which of the following is MOST helpful to developing a comprehensive Information security strategy?
A. Performing a business impact analysts (BIA).
B. Conducting a risk assessment
C. Adopting an industry framework
D. Gathering business objectives
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
When reporting on the effectiveness of the information security program, which of the following is the BEST way lo demonstrate improvement m security performance?
A. Present a penetration testing report conducted by a third party
B. Benchmark security metrics against industry standard
C. Report the results of a security control self-assessment (CSA).
D. Provide a summary of security project return on investments (ROIs) for the past year.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
An information security manager determines the organizations critical systems may be vulnerable to a new zero-day attack. The FIRST course of action is to:
A. advise management of risk and remediation cost
B. analyze the probability of compromise
C. re-assess the firewall configuration
D. survey peer organizations to see how they have addressed the issue.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 142
To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:
A. assess the risks of all new equipment.
B. ensure compliance during user acceptance testing.
C. assess security during equipment deployment.
D. develop an approved equipment list.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
Which of the following will provide the MOST accurate test results for a disaster recovery plan (DRP)?
A. Simulation test
B. Parallel test
C. Structured walk-through

D. Full interruption test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
Which of the following is the PRIMARY reason for performing an analysis of the threat landscape on a regular basis?
A. To determine if existing business continuity plans are adequate
B. To determine the basis for proposing an increase in security budgets
C. To determine critical information for executive management
D. To determine if existing vulnerabilities present a risk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
Which of the following BEST demonstrates effective information security management within an organization?
A. Control ownership is assigned to parties who can accept losses related to control failure.
B. Employees support decisions made by information security management.
C. Information security governance is incorporated into organizational governance.
D. Excessive risk exposure in one department can be absorbed by other departments.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 146
Which of the following is an example of a change to the external threat landscape?
A. New legislation has been enacted in a region where the organization does business.
B. Organizational security standards have been modified.
C. Infrastructure changes to the organization have been implemented.
D. A commonly used encryption algorithm has been compromised.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 147
When reporting to senior management on an information security vulnerability that could lead to a potential breach, what information is MOST likely to facilitate the decision-making process?
A. Business impact
B. Cost to remediate
C. Risk treatment options
D. Regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 148

Which of the following is the MOST important reason for an organization to develop an information security governance program?
A. Establishment of accountability
B. Monitoring of security incidents
C. Creation of tactical solutions
D. Compliance with audit requirements
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following should be the FIRST course of action when it becomes apparent that the recovery time objective (RTO) will not be met during incident response
A. Request additional financial recovery resources.
B. Notify the risk management team.
D Modify the RTO as needed
C. Escalate the emergency status rating.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
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: A (LEAVE A REPLY)

NEW QUESTION: 151
Which of the following is the MOST important criterion for complete closure of a security incident?
A. Documenting and reporting to senior management
B. Level of potential impact
C. Identification of affected resources
D. Root cause analysis and lessons learned
Answer: D (LEAVE A REPLY)

NEW QUESTION: 152
Which of the following should provide the PRIMARY basis for formulating an information security strategy?
A. The regulatory environment
B. The IT strategy
C. The information security framework
D. The business strategy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 153
Which of the following activities should take place FIRST when a security patch for Internet software is received from a vendor?
A. The patch should be deployed quickly to systems that are vulnerable.
B. The patch should be validated using a hash algorithm.
C. The patch should be applied to critical systems.
D. The patch should be evaluated in a testing environment.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
A newly appointed Information security manager finds mere is minimal interaction between departments in identifying ...risk due to the organization's current decentralized structure What is the managers BEST course of action?
A. identify appropriate risk management training for relevant staff in the departments
B. Propose the creation of a consolidated organizational risk register to track risk
C. Recommend consolidating all risk management activities under a central authority.
D. Modify the current practices within the governance framework.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 155
What should be information security manager's FIRST course of action when it is discovered a staff member has been posting corporate information on social media sites?
A. Notify senior management
B. Implement controls to block the social media sites.
C. Refer the staff member to the information security policy
D. Asses the classification of the data posted.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 156

Which of the following BEST supports effective information security governance"*

A. Compliance with regulations is demonstrated.

B. The information security manager develops the strategy

C. A baseline risk assessment is performed.

D. A steering committee is established

Answer: (SHOW ANSWER)

NEW QUESTION: 157

Which of the following would BEST demonstrate the maturity level of an organization's security incident response program?

A. An increase in the number of reported incidents

B. A decrease in the number of reported incidents

C. Ongoing review and evaluation of the incident response team

D. A documented and live-tested incident response process

Answer: (SHOW ANSWER)

NEW QUESTION: 158

Which of the following BEST demonstrates the effectiveness of the vulnerability management process?

A. Results of third-party penetration testing

B. Resource allocation for remediating vulnerabilities

C. Average time from patch release to catch installation

D. Performance of periodic internal vulnerability scans

Answer: (SHOW ANSWER)

NEW QUESTION: 159

Which of the following should an information security manager establish FIRST to ensure security-related activities are adequately monitored?

A. Regular reviews of computer system logs

B. Accountability for security functions

C. Scheduled security assessments

D. Internal reporting channels

Answer: (SHOW ANSWER)

NEW QUESTION: 160

Noncompliance issues were identified through audit. Which of the following is the BEST approach for the information security manager to ensure that issues are resolved in a timely manner?

A. Collaborate with the business process owner to implement mitigation controls.

B. Escalate the noncompliance issues to senior management

C. Perform a risk assessment.

D. Develop a solution independently
Answer: A (LEAVE A REPLY)

NEW QUESTION: 161
Which of the following would BEST ensure that application security standards are in place?
A. Penetration testing
B. Functional testing
C. Performing a code review
D. Publishing software coding standards
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
Which of the following BEST measures the effectiveness of an organization's information security strategy?
A. Comparison of threats to vulnerabilities
B. Comparison of mitigated risk to accepted risk
C. Comparison of current security budget to previous year's budget
D. Comparison of residual risk to risk appetite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following should an information security manager do FIRST when an organization plans to migrate all internally hosted applications to the cloud?
A. Assess the risk associated with the cloud services.
B. Determine information security requirements for the cloud.
C. Develop key risk indicators (KRIs).
D. Create an information security action plan.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
What should be an information security manager's BEST course of action if funding for a security-related initiative is denied by a steering committee?
A. Look for other ways to fund the initiative.
B. Provide information from industry benchmarks
C. Document the accepted risk
D. Discuss the initiative with senior management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Which of the following is MOST important for an information security manager to highlight when presenting the organization s security posture to an executive audience?

A. Published sophisticated security threats targeting the Industry
B. The number of emails blocked by the data loss prevention (DLP) system
C. Security risks that may inhibit business objectives
D. Performance metrics specific to business urn! security awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Application data integrity risk would be MOST directly addressed by a design that includes:
A. strict application of an authorized data dictionary.
B. reconciliation routines such as checksums, hash totals, and record counts
C. access control technologies such as role-based entitlements.
D. application log requirements such as field-level audit trails and user activity logs.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
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. Survey end users about corporate governance.
D. Evaluate funding for security initiatives.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 168
What is the PRIMARY purpose of communicating business impact to an incident response team?
A. To facilitate resource allocation tor preventive measures
B. To provide information for communication of incidents
C. To enable effective prioritization of incidents
D. To provide monetary values for post-incident review
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
In an organization that has undergone an expansion through an acquisition, which of the following would BEST secure the enterprise network?
A. Using security groups
B. Log analysis of system access
C. Business or rote-based segmentation
D. Encryption of data traversing networks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
When preparing a strategy for protection from SQL injection attacks, it is MOST important for the information security manager to involve:
A. application developers.
B. the security operations center.
C. senior management.
D. business owners.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 171
Which of the following is the MOST effective way for an information security manager to protect the organization from misuse of social media?
A. Hire a social media manager to control content delivered via social media.
B. Deliver regular social media awareness training to all employees.
C. Scan social media platforms for company references
D. Restrict the use of social media on corporate networks and devices
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which of the following helps to ensure that the appropriate resources are applied in a timely manner after an incident has occurred?
A. Initiate an incident management log
B. Broadcast an emergency message
C. Classify the incident
D. Define incident response teams.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 173
Which of the following is the GREATEST benefit of information asset classification?
A. Providing a basis for implementing a need-to-know policy
B. Supporting segregation of duties
C. Defining resource ownership

D. Helping to determine the recovery point objective (RPO)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 174
An information security manager suspects that the organization has suffered a ransomware attack. What should be done FIRST
A. Notify senior management
B. Alert employees to the attack.
C. Isolate the affected systems.
D. Confirm the infection.
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which of the following is MOST important when selecting an information security metric?
A. Aligning the metric to the IT strategy
B. Defining the metric in qualitative terms
C. Defining the metric in quantitative terms
D. Ensuring the metric is repeatable
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Which of the following is the PRIMARY purpose of establishing an information security governance framework?
A. To enhance business continuity planning
B. To minimize security risks
C. To reduce security audit issues
D. To proactively address security objectives
Answer: D (LEAVE A REPLY)

NEW QUESTION: 177
Following a highly sensitive data breach at a large company, all servers and workstations were patched. The information security manager s NEXT step should be to:
A. ensure baseline back-ups are performed.
B. perform an assessment to measure the current state
C. inform senior management of changes in risk metrics.
D. deliver security awareness training.
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which of the following would BEST ensure thai security risk assessment is integrated into the life cycle of major IT projects

A. Training project managers on risk assessment
B. Having the Information security manager participate on the project steering committees
C. Integrating the risk assessment into the internal audit program
D. Applying global security standards to the IT projects
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?
A. Defined security standards
B. Regular antivirus updates
C. Threat intelligence
D. Updated security policies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 180
An organization is considering whether to allow employees to use personal computing devices for business purposes To BEST facilitate senior management's decision, the information security manager should:
A. conduct a risk assessment.
B. map the strategy to business objectives.
D, perform a cost-benefit analysis.
C. develop a business case.
Answer: (SHOW ANSWER)

NEW QUESTION: 181
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 combination of qualitative and quantitative trends that enable decision making
C. The number of key risk indicators (KRIs) identified, monitored, and acted upon
D. A single numeric score derived from various measures assigned to the security program
Answer: (SHOW ANSWER)

NEW QUESTION: 182
Which of the following is the BEST method to defend against social engineering attacks?
A. Employ the use of a web-content filtering solution.
B. Periodically perform antivirus scans to identify malware
C. Communicate guideline to limit information posted to public sites
D. Monitor for unauthorized access attempts and failed logins.
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which of the following would be MOST effective in preventing malware from being launched through an email attachment?
A. Up-to-date security policies
B. A network intrusion detection system (NIDS)
C. Security awareness training
D. Placing the e-mail server on a screened subnet
Answer: C (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following is the MOST important reason to consider the role of the IT service desk when developing incident handling procedures?
A. Service desk personnel have information on how to resolve common systems issues
B. Untrained service desk personnel may be a cause of security incidents.
C. The service desk provides information to prioritize systems recovery based on user demand
D. The service desk provides a source for the identification of security incidents.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
Which of the following is MOST important to include in contracts with key third-party providers?
A. Right-to-terminate clauses
B. Financial penalties for breaches
C. Right-to-audit clauses
D. Provisions to protect sensitive data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 186

An online payment provider's computer security incident response team has confirmed that a customer credit card database was breached. Which of the following would be MOST important to include in a report to senior management?
A. A summary of the security togs illustrating the sequence of events
B. An explanation of the potential business impact
C. An analysis of similar attacks and recommended remediation
D. A business case for implementing stronger logical access controls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
Which of the following is the BEST way to measure the effectiveness of a newly implemented social engineering training program?
A. Track the trending of reported security incidents
B. Track the trending of malware infections.
C. Administer quizzes upon completion of training.
D. Test end user response to simulated scenarios
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
Which of the following is the MOST important delivery outcome of information security governance?
A. Vulnerability assessment
B. Strategic alignment
C. Asset protection
D. Data classification
Answer: (SHOW ANSWER)

NEW QUESTION: 189
Which of the following is MOST important to consider when determining the effectiveness of the Information security governance program?
A. Key performance indicators (KPIs)
B. Key risk indicators (KRIs)
C. Maturity models
D. Risk tolerance levels
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following is MOST likely to occur following a security awareness campaign"
A. A decrease in user-reported false positive incidents
B. An increase in the number of viruses detected in incoming email
C. A decrease in number of account lockouts

D. An increase in reported social engineering attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 191
An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's FIRST course of action?
A. Inform respective risk owners of the impact of exceptions.
B. Prioritize the risk and implement treatment options.
C. Report the noncompliance to the board of directors.
D. Design mitigating controls for the exceptions.
Answer: (SHOW ANSWER)

NEW QUESTION: 192
A business unit has updated its long-term business plan to include a strategy of upgrading information management system to increase productivity. To support this initiative, with the information security strategy?
A. The business strategy
B. The IT strategy
C. the information security framework
D. It risk assessment results
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the BEST assurance that the third party's contract programmers comply with the organization's security policies?
A. Conduct periodic vulnerability scans of the application.
B. Include penalties for noncompliance in the contracting agreement.
C. Perform periodic security assessments of the contractors' activities.
D. Require annual signed agreements of adherence to security policies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
Which of the following is BEST performed by the security department?
A. Provisioning users to access the operating system
B. Managing user profiles for accessing the operating system
C. Logging unauthorized access to the operating system
D. Approving standards for accessing the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 195
Which of the following is the STRONGEST indication that senior management commitment to information security is lacking within an organization?
A. A reduction in information security investment
B. The information security manager reports to the chief risk officer
C. A high level of information security risk acceptance
D. Inconsistent enforcement of information security policies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 196
Which of the following is the MOST effective method of preventing deliberate internal security breaches?
A. Biometric security access control
B. Screening prospective employees
C. Well-designed firewall system
D. Well-designed intrusion detection system (IDS)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 197
Which of the following is a benefit of using key risk indicators (KRIs)?
A. Reduction in the annual loss expectancy (ALE)
B. Determination of the residual risk value
C. Ability to analyze risk trends
D. Support for the incident response process
Answer: (SHOW ANSWER)

NEW QUESTION: 198
An information security manager is reviewing the business case for a security project that is entering the development phase It is determined that the estimates cost of the controls is now greater than the risk being mitigated. What is the information security manager's BEST recommendation?

A. Pursue the project until the benefits cover the costs.
B. Discontinue the project to release funds for other efforts
C. Slow the pace of the project to spread costs over a longer period.
D. Eliminate some of the controls from the project scope.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 199
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 activity----
A. Determine alternative controls.
B. Accept the risk and document the exception.
C. Investigate alternative mobile applications.
D. Modify the policy to accommodate the application capabilities.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
An organization is MOST at risk from a new worm being introduced through the intranet when:
A. desktop virus definition files are not up to date
B. executable code is run from inside the firewall
C. system software does not undergo integrity checks.
D. hosts have static IP addresses.
Answer: (SHOW ANSWER)

NEW QUESTION: 201
Which of the following is the MOST important criterion when deciding whether to accept residual risk?
A. Annual rate of occurrence (ARO)
B. Cost of additional mitigation
C. Annual loss expectancy (ALE)
D. Cost of replacing the asset
Answer: D (LEAVE A REPLY)

NEW QUESTION: 202
A business unit manager wants to adopt an emerging technology that may affect the organization. Which of the following would be the information security manager's BEST course of action?
A. Review vendor documentation.
B. Review the business case.
C. Perform a business impact analysis (BIA).

D. Perform a threat analysis.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 203
The PRIMARY purpose of a risk assessment is to enable business leaders to:
A. define key risk indicators (KRIs).
B. align information security to business objectives.
C. make informed decisions.
D. manage information security expenditures.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 204
Which of the following is MOST critical when creating an incident response plan?
A. identifying vulnerable data assets
B. Documenting incident notification and escalation processes
C. identifying what constitutes an incident
D. Aligning with the risk assessment process
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205
Which of the following external entities would provide the BEST guideance to an organization facing advanced attacks?
A. Incident response experts from highly regarded peer organizations
B. Disaster recovery consultants widely endorsed in industry forums
C. Recognised threat intelligence communities
D. Open-source reconnaissance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
Which of the following tools BEST demonstrates the effectiveness of the information security program?
A. Key risk indicators (KRIs)
B. A security balanced scorecard
C. Risk heat map
D. Management satisfaction surveys
Answer: A (LEAVE A REPLY)

NEW QUESTION: 207
An information security manager has determined that the mean time to prioritize information security incidents has increased to an unacceptable level. Which of the

following processes would BEST enable the information security manager to address this concern?

A. Forensic analysis

B. Incident response

C. Incident classification

D. Vulnerability assessment

Answer: C (LEAVE A REPLY)

NEW QUESTION: 208

An information security manager has been made aware that implementing a control would have an adverse impact to the business. The business manager has suggested accepting the risk. The BEST course of action by the information security manager would be to:

A. continue implementing the control.

B. review existing technical controls.

C. document the risk exception

D. recommend compensating controls

Answer: (SHOW ANSWER)

NEW QUESTION: 209

The MOST effective way to continuously monitor an organization's cybersecurity posture is to evaluate its

A. level of support from senior management.

B. key performance indicators (KPIs).

C. timeliness m responding to attacks.

D. compliance with industry regulations.

Answer: (SHOW ANSWER)

NEW QUESTION: 210

An information security manager learns users of an application are frequently using emergency elevated access privileges to process transactions Which of the following should be done FIRST?

A. Request the application administrator block all emergency access profiles.

B. Request justification from the users managers for emergence access

C. Review the security architecture of the application and recommend changes

D. Update the frequency and usage of the emergency access profile in the policy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 211

Which of the following is the BEST mechanism to prevent data loss in the event personal computing equipment is stolen or lost?

A. Data encryption

B. Data leakage prevention (DLP)
C. Personal firewall
D. Remote access to device
Answer: (SHOW ANSWER)

NEW QUESTION: 212
The FIRST step in a risk assessment for a business application is to:
A. identify the assets used by the application.
B. identify the vulnerabilities of the application
C. identify the threats to the application
D. rank the threats to the application
Answer: A (LEAVE A REPLY)

NEW QUESTION: 213
An internal security audit has reported that authentication controls are not operating effectively. Which of the following is MOST important to c management?
A. A business case for implementing stronger authentication controls
B. The impact of the control weakness on the risk profile of the organization
C. An analysis of the impact of this type of control weakness on other organizations
D. The results of a business impact analysis (BIA)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 214
Which of the following would BEST enhance firewall security?
A. Logging of security events
B. Implementing change-control practices
C. Providing dynamic address assignment
D. Placing the firewall on a screened subnet
Answer: (SHOW ANSWER)

NEW QUESTION: 215

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

NEW QUESTION: 216
Which of the following should be done FIRST when considering a new security initiative?
A. Perform a cost-benefit analysis.
B. Conduct a benchmarking exercise.
C. Conduct a feasibility study.
D. Develop a business case.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
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. assess alignment with business objectives.
B. perform a risk assessment
C. implement two-factor authentication.
D. escalate the request to senior management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 218
Which of the following is the FIRST step to promoting acceptable behavior with regard to information security throughout an organization?
A. Require signed acknowledgment of acceptable use policies.
B. Incorporate information security standards into performance evaluations.
C. Automate controls that enforce acceptable use.
D. Conduct targeted acceptable use training for management and staff.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 219
Which of the following should be the information security manager's NEXT step following senior management approval of the information security strategy?
A. Develop a budget
B. Perform a gap analysis.
C. Develop a security pokey.

D. Form a steering committee
Answer: D (LEAVE A REPLY)

NEW QUESTION: 220
When responding to an incident, which of the following is required to ensure evidence remains legally admissible in court?
A. A documented incident response plan
B. Certified forensics examiners
C. Chain of custody
D. Law enforcement oversight
Answer: C (LEAVE A REPLY)

NEW QUESTION: 221
Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?
A. Ratio of successful to unsuccessful tests
B. Ratio of tested applications to total applications
C. Number of published application-recovery plans
D. Ratio of recovery-plan documents to total applications
Answer: (SHOW ANSWER)

NEW QUESTION: 222
Which of the following is the BEST approach when using sensitive customer data during the testing phase of a systems development project?
A. Establish the test environment on a separate network.
B. Implement equivalent controls to those on the source system
C. Sanitize customer data.
D. Monitor the test environment for data loss.
Answer: (SHOW ANSWER)

NEW QUESTION: 223
Which of the following should the information security manager do FIRST after a security incident has been reported?
A. Identify the possible source of attack.
B. Determine the degree of loss resulting from the incident.
C. Identify the scope and size of the affected environment.
D. Retrieve the information needed to confirm the incident.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 224

Key systems necessary for branch operations reside at corporate headquarters. Branch A is negotiating with a third party to provide disaster recovery facilities. Which of the following contract terms would be the MOST significant concern?
A. Connectivity Is not provided from the hot site to corporate headquarters.
B. The right to audit the hot site Is not provided In the contract.
C. Penalty clauses for nonperformance are not included in the contract
D. The hot site for the branch may have to be shared.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
When trying to integrate information security across an organization, the MOST important goal for a governing body should be to ensure:
A. periodic information security audits are conducted.
B. information security is treated as a business critical issue.
C. the resources used for information security projects are kept to a minimum.
D. funding is approved for requested information security projects.
Answer: (SHOW ANSWER)

NEW QUESTION: 226
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. Provide an analysis of current risk exposures.
B. Provide the estimated return on investment (ROI).
C. Include historical data of reported incidents.
D. Include industry benchmarking comparisons.
Answer: (SHOW ANSWER)

NEW QUESTION: 227
The MOST important reason that security risk assesements should be conducted frequently through an organization is because:
A. Control effectiveness may weaken.

B. Compliance with legal and regulatory should be reassessed.
C. Threats to the organization may change
D. Controls should be regularly tested.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 228
Which of the following should be reviewed to obtain a structured overview of relevant information about an information security investment?
A. Security balanced scorecard
B. Quantitative risk analysis report
C. Business case
D. Information security strategy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
To meet operational business needs. IT staff bypassed the change process and applied an unauthorized update to a critical business system Which of the following is the information security manager's BEST course of action?
A. Instruct IT staff to revert the unauthorized update
B. Update the system configuration item to reflect the change
C. Assess the security risks introduced by the change.
D. Consult with supervisors of IT staff regarding disciplinary action
Answer: (SHOW ANSWER)

NEW QUESTION: 230
Which of the following is the MOST effective way for an organization to ensure its third-party service providers are aware of information security requirements and expectations?
A. Requiring third parties to sign confidentiality agreements
B. Inducting information security clauses within contracts
C. Auditing the service delivery of third-party providers
D. Providing information security training to third-party personnel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 231
Which of the following is the MOST important factor to consider when establishing a severity hierarchy for information security incidents?
A. Management support
B. Residual risk
C. Business impact
D. Regulatory compliance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 232
An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the information security manager?
A. Follow the outsourcers response plan.
B. Alert the appropriate law enforcement authorities.
C. Notify the outsourcer of the privacy breach.
D. Refer to the organization's response plan.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 233
Which of the following poses the GREATEST risk to the operational effectiveness of an incident response team?
A. The lack of delegated authority
B. The lack of automated communication channels
C. The lack of forensic investigation skills
D. The lack of a security information and event management (SIEM) system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 234
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. Password carelessness by one user may render the entire infrastructure vulnerable
C. Integration of single sign-on with the rest of the infrastructure is complicated
D. One administrator maintains the single sign-on solutions without segregation of duty.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 235
Which of the following is the MOST important reason to document information security incidents that are reported across the organization?
A. Evaluate the security posture of the organization.
B. Prevent incident recurrence.
C. Support business investments in security
D. Identify unmitigated risk.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
Which of the following is MOST relevant for an information security manager to communicate to the board of directors?
A. Threat assessments

B. Vulnerability assessments
C. The level of exposure
D. The level of inherent risk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 237
Senior management wants to provide mobile devices to its sales force. Which of the following should the Information security manager do FIRST to support this objective?
A. Develop an acceptable use policy.
B. Research mobile device management (MDM) solutions.
C. Assess risks introduced by the technology
D. Conduct a vulnerability assessment on the devices.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 238
Which of the following is the MOST important consideration when designing information security architecture?
A. The existing threat landscape is monitored.
B. The information security architecture is aligned with industry standards.
C. The level of security supported is based on business decisions.
D. Risk management parameters for the organization are defined.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 239
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. Perform a gap analysis
B. Interview senior management
C. Conduct a risk assessment
D. Conduct a cost-benefit analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 240
In the development of an information security strategy, recovery time objectives (RTOs) will serve as indicators of:
A. open vulnerabilities.
B. risk tolerances.
C. maturity levels.
D. senior management support.
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Which of the following is the MOST important consideration when updating procedures for managing security devices?
A. Updates based on the organization's security framework
B. Notification to management of the procedural changes
C. Review and approval of procedures by management
D. Updates based on changes in risk, technology, and process
Answer: (SHOW ANSWER)

NEW QUESTION: 242
Which of the following will BEST facilitate the understanding of information security responsibilities by users across the organization?
A. Conducting security awareness training with performance incentives
B. Incorporating information security into the organization's code of conduct
C. Communicating security responsibilities as an acceptable usage policy
D. Warning users that disciplinary action will be taken for violations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
Which of the following is the MOST important consideration of the information security manager to ensure effective security monitoring of outsourced operations?
A. Performing security audits on the outsourcing vendor s IT environment
B. Monitoring security incidents and periodic security reports from the outsourcing vendor
C. Reflecting monitoring requirements m the contractual indemnity agreement
D. including security requirements and right to audit within the contract
Answer: D (LEAVE A REPLY)

NEW QUESTION: 244
Which of the following is the BEST indication that a recently adopted information security framework is a good fit for an organization?
A. The business has obtained framework certification.
B. Objectives in the framework correlate directly to business practices

C. The framework includes industry-recognized information security best practices.
D. The number of security incidents has significantly declined
Answer: B (LEAVE A REPLY)

NEW QUESTION: 245
Failure to include information security requirements within the build/buy decision would MOST likely result in the need for:
A. compensating controls in the operational environment.
B. commercial product compliance with corporate standards.
C. more stringent source programming standards.
D. security scanning of operational platforms
Answer: A (LEAVE A REPLY)

NEW QUESTION: 246
Which of the following is the MAIN concern when securing emerging technologies?
A. Compatibility with legacy systems
B. Integrating with existing access controls
C. Applying the corporate hardening standards
D. Unknown vulnerabilities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 247
An access rights review revealed that some former employees' access is still active. Once the access is revoked, which of the following is the BEST course of action to help prevent recurrence?
A. Conduct a root cause analysis.
B. Initiate an access control policy review.
C. Implement a periodic recertification program.
D. Validate HR offboarding processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 248
Information security governance is PRIMARILY driven by which of the following?
A. Technology constraints
B. Regulatory requirements
C. Litigation potential
D. Business strategy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
What is a potential issue when emails are encrypted and digitally signed?

A. The receiver can repudiate the receipt of the emails.
B. The sender can repudiate the contents of the emails.
C. Hackers can introduce forged messaging within emails.
D. Hackers can eavesdrop on emails.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 250
Exceptions to a security policy should be approved based PRIMARILY on:
A. risk appetite.
B. the external threat probability.
C. results of a business impact analysis (BIA).
D. the number of security incidents.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 251
Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?
A. The ability to meet deliverables
B. The business need for the function
C. The cost of the services
D. The vendor's reputation m the industry
Answer: (SHOW ANSWER)

NEW QUESTION: 252
Which of the following provides the MOST relevant evidence of incident response maturity?
A. Average incident closure time
B. Independent audit assessment
C. Red team testing results
D. Tabletop exercise results
Answer: (SHOW ANSWER)

NEW QUESTION: 253
When creating an incident response plan, the PRIMARY benefit of establishing a clear definition of a security incident is that it helps to:
A. communicate the incident response process to stakeholders
B. develop effective escalation and response procedures.
C. adequately staff and train incident response teams.
D. make tabletop testing more effective.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 254
Which of the following would provide nonrepudiation of electronic transactions?
A. Receipt acknowledgment
B. Two-factor authentication
C. Third-party certificates
D. Periodic reaccreditations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 255
The MOST important reason to have a well-documented and tested incident response plan in place is to:
A. facilitate the escalation process
B. promote a coordinated effort
C. outline external communications
D. standardize the chain of custody procedure.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 256
Which of the following is the GREATEST benefit of information asset classification to an organization?
A. It demonstrates the value of information assets for financial reporting.
B. It measures qualitative value of the information.
C. It helps to optimize the investment in protecting information assets.
D. It helps to minimize the cost of regulatory compliance efforts
Answer: C (LEAVE A REPLY)

NEW QUESTION: 257
Which of the following should be an information security manager's MOST important consideration when determining if an information asset has been classified appropriate.
A. Value to the business
B. Security policy requirements
C. Ownership of information

D. Level of protection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 258
The authorization to transfer the handling of an internal security incident to a third-party support provider is PRIMARILY defined by the:
A. information security manager
B. disaster recovery plan (DRP)
C. escalation procedures
D. chain of custody.
Answer: (SHOW ANSWER)

NEW QUESTION: 259
When management changes the enterprise business strategy, which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?
A. Access control management
B. Change management
C. Configuration management
D. Risk management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 260
During a post-incident review, the sequence and correlation of actions must be analyzed PRIMARILY based on:
A. logs from systems involved.
B. a consolidated event timeline
C. interviews with personnel.
D. documents created during the incident.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 261
Which of the following is the MOST effective method to prevent a SQL injection in an employee portal?
A. Enforce referential integrity on the database.
B. Reconfigure the database schema.
C. Conduct network penetration testing.
D. Conduct code reviews.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 262

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

NEW QUESTION: 263
Which of the following is an information security manager's BEST course of action when informed of decision to reduce funding for the information security program?
A. Design key risk indicators (KRIs)
B. Create a business case appeal decision.
C. Prioritize security projects based on risk.
D. Remove overlapping security controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 264
Which of the following is the PRIMARY purpose of red team testing?
A. To confirm the risk profile of the organization
B. To determine the organization s preparedness for an attack
C. To assess the vulnerability of employees to social engineering
D. To establish a baseline incident response program
Answer: (SHOW ANSWER)

NEW QUESTION: 265
The PRIMARY reason for using information security metrics is to:
A. adhere to legal and regulatory requirements
B. achieve senior management commitment.
C. monitor the effectiveness of controls
D. ensure alignment with corporate requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 266
Which of the following is the MOST important outcome from vulnerability scanning?
A. Identification of back doors
B. Verification that systems are property configured
C. Prioritization of risks
D. Information about steps necessary to hack the system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 267

Which of the following is the PRIMARY reason an information security strategy should be deployed across an organization?
A. To ensure that employees adhere to security standards
B. To ensure that management's intent is reflected in security activities
C. To ensure that the business complies with security regulations
D. To ensure that security-related industry best practices are adopted
Answer: (SHOW ANSWER)

NEW QUESTION: 268
Which of the following enables compliance with a nonrepudiation policy requirement for electronic transactions?
A. One-time passwords
B. Digital certificates
C. Encrypted passwords
D. Digital signatures
Answer: (SHOW ANSWER)

NEW QUESTION: 269
After a recent malware Incident an organization's IT steering committee has asked the information security manager for a presentation on the status of the information security program. Which of the following is MOST important to address in the presentation?
A. Disaster recovery and continuity program plans
B. Measures taken to prevent the risk of a data breach
C. Antivirus program and incident response plans
D. Remediation schedule for patch management
Answer: (SHOW ANSWER)

NEW QUESTION: 270
Which of the following is the MOST effective preventive control?
A. Review of audit logs
B. Restoration of a system from backup
C. Warning banners on login screens
D. Segregation of duties
Answer: D (LEAVE A REPLY)

NEW QUESTION: 271
Which of the following is MOST helpful for aligning security operations with the IT governance framework?
A. Business impact analysis (B1A)
B. Security risk assessment
C. Information security policy

D. Security operations program
Answer: (SHOW ANSWER)

NEW QUESTION: 272
The BEST way 10 establish a security baseline is by documenting
A. a framework of operational standards
B. the organization's preferred security level.
C. a standard of acceptable settings
D. the desired range of security settings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 273
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. Send periodic fake phishing emails to employees and track responses.
D. Conduct information security awareness training for employees.
Answer: (SHOW ANSWER)

NEW QUESTION: 274
An organization has announced new initiatives to establish a big data platform and develop mobile apps. What is the FIRST step when defining new human resource requirements?
A. Analyze the skills necessary to support the new initiatives.
B. Determine the security technology requirements for the initiatives
C. Benchmark to an industry peer
D. Request additional funding for recruiting and training
Answer: (SHOW ANSWER)

NEW QUESTION: 275

Which of the following MOST effectively helps an organization to align information security governance with corporate governance?

A. Adopting global security standards to achieve business goals

B. Developing security performance metrics

C. Promoting security as enabler 10 achieve business objectives

D. Prioritizing security initiatives based on IT strategy

Answer: C (LEAVE A REPLY)

NEW QUESTION: 276

Which of the following provides the BEST justification for an information security investment when creating a business case

A. The investment can be managed using the organisation's established system development life cycle.

B. The investment reduces the protected asset s inherent risk below the asset s residual risk

C. The annualized loss expectancy (ALE) is greater than the annual cost of the investment.

D. Key risk indicators (KRIs) are available to measure the effectiveness and efficiency of the investment

Answer: C (LEAVE A REPLY)

NEW QUESTION: 277

Which of the following should be the FIRST step to ensure system updates are applied in a timely manner?

A. Create a regression test plan to ensure business operation is not interrupted.

B. Run a patch management scan to discover which patches are missing from each machine.

C. Establish a risk-based assessment process for prioritizing patch implementation.

D. Cross-reference all missing patches to establish the date each patch was introduced.

Answer: (SHOW ANSWER)

NEW QUESTION: 278

Which of the following is the PRIMARY objective of implementing an information security strategy?

A. To maintain adherence to information security policies

B. To align with industry best practices

C. To manage risk to an acceptable level

D. To demonstrate compliance with legal requirements

Answer: C (LEAVE A REPLY)

NEW QUESTION: 279

Which of the following approaches would MOST likely ensure that risk management is integrated into the business life cycle processes?
A. Integrating security risk into corporate risk management
B. Conducting periodic risk assessments
C. Integrating risk management into the software development life cycle
D. Understanding the risk tolerance of corporate management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 280
Which of the following is an indicator of improvement in the ability to identify security risks?
A. Decreased number of information security risk assessments
B. Increased number of security audit issues resolved
C. Increased number of reported security incidents
D. Decreased number of staff requiring information security training
Answer: C (LEAVE A REPLY)

NEW QUESTION: 281
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:
A. review the state of security awareness.
B. perform a gap analysis.
C. perform a risk assessment
D. review information security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 282
Which of the following processes would BEST help to ensure that information security risks will be evaluated when implementing a new payroll system?
A. Change management
B. Configuration management
C. Incident management
D. Problem management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
Which of the following would BEST help to ensure an organization's information security strategy is aligned with business objectives?
A. Establishing a change control process for continued updating of security policies
B. Establishing metrics to measure the effectiveness of the information security program
C. Requesting senior management to periodically review security incidents
D. Implementing an automated solution for monitoring information security processes

Answer: C (LEAVE A REPLY)

NEW QUESTION: 284
Which of the following is the MOST important consideration when developing an incident management program?
A. Impact assessment
B. Escalation procedures
C. IT architecture
D. Risk assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 285
Which of the following is the MOST important function of information security?
A. Preventing security incidents
B. Managing risk to the organization
C. Identifying system vulnerabilities
D. Reducing the financial impact of security breaches
Answer: B (LEAVE A REPLY)

NEW QUESTION: 286
In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOS important for the information security manager to ensure:
A. compliance with the risk acceptance framework
B. change activities are documented
C. the acceptance is aligned with business strategy.
D. the rationale for acceptance is periodically reviewed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 287
To ensure adequate disaster-preparedness among IT infrastructure personnel, it is MOST important to:

A. periodically rotate recovery-test participants.
B. assign personnel-specific duties in the recovery plan.
C. have the most experienced personnel participate in recovery tests.
D. include end-user personnel in each recovery test.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 288
The selection of security controls is PRIMARILY linked to:
A. risk appetite of the organization.
B. best practices of similar organizations.
C. business impact assessment
D. regulatory requirements
Answer: C (LEAVE A REPLY)

NEW QUESTION: 289
An information security manager is asked to provide a short presentation on the organization's current IT risk posture to the board of directors. Which of the following would be MOST effective To include in this presentation?
A. Risk heat map
B. Risk register
C. Threat assessment results
D. Gap analysis results
Answer: D (LEAVE A REPLY)

NEW QUESTION: 290
Which of the following is the MOST reliable source of information about emerging information security threats and vulnerabilities?
A. Threat intelligence groups
B. Vulnerability scanning alerts
C. Industry bloggers
D. A social media group of hackers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 291
The PRIMARY objective for using threat modeling in web application development should be to:
A. review application source code.
B. build security into the design.
C. develop application development standards.
D. determine if penetration testing is necessary.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 292
Which of the following would provide the MOST helpful information when developing a prioritized list of IT assets to protect in the event of an incident?
A. The service level agreement (SLA) for the IT asset
B. The owner of the IT asset
C. The classification of the information processed by the IT asset
D. The replacement cost of the IT asset
Answer: C (LEAVE A REPLY)

NEW QUESTION: 293
Which of the following is the information security manager's PRIMARY role in the information assets classification process?
A. Assigning asset ownership
B. Assigning the asset classification level
C. Securing assets in accordance with their classification
D. Developing an asset classification model
Answer: C (LEAVE A REPLY)

NEW QUESTION: 294
An information security manager is developing evidence preservation procedures for an incident response plan. Which of the following would be the BEST source of guidance for requirements associated with the procedures?
A. IT management
B. Legal counsel
C. Executive management
D. Data owners
Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
Which of the following is the MOST appropriate board-level activity for information security governance?
A. Establish measures for security baselines.
B. Develop 'what-if' scenarios on incidents
C. Include security in job performance appraisals
D. Establish security and continuity ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 296
Cold sites for disaster recovery events are MOST helpful in situations in which a company:
A. uses highly specialized equipment that must be custom manufactured.

B. does not require any telecommunications connectivity.
C. has a limited budget for coverage.
D. is located in close proximity to the cold she.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
An organization is considering moving lo a cloud service provider for the storage of sensitive data Which of the following .... consideration FIRST?
A. A destruction-of-data clause m the contract
B. Requirements for data encryption
C. Results of the cloud provider's control report
D. Right to terminate clauses In the contract
Answer: B (LEAVE A REPLY)

NEW QUESTION: 298
Which of the following is the BEST method for management to obtain assurance of compliance with its security policy?
A. Question staff concerning their security duties.
B. Review security incident logs.
C. Conduct regular independent reviews.
D. Train staff on their compliance responsibilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 299
The PRIMARY objective of a risk response strategy should be:
A. threat reduction.
B. appropriate control selection.
C. regulatory compliance.
D. senior management buy-in.
Answer: (SHOW ANSWER)

NEW QUESTION: 300
The integration of information security risk management processes within corporate risk management processes will MOST likely result in:
A. information security controls that reduce enterprise risk.
B. senior management approval of the information security budgets.
C. more effective security risk management processes.
D. improved efficiencies of security operations.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 301

Which of the following should be done FIRST when handling multiple confirmed incidents raised at the same time?
A. Activate the business continuity plan (BCP).
B. Inform senior management.
C. Update the business impact assessment.
D. Categorize incidents by the value of the affected asset.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 302
Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?
A. Integrate industry best practices.
B. Conduct an organization-wide security audit.
C. Obtain senior management sign-off.
D. Leverage security steering committee contribution.
Answer: (SHOW ANSWER)

NEW QUESTION: 303
A multinational organization wants to ensure its privacy program appropriately addresses privacy risk throughout its operations. Which of the following would be of MOST concern to senior management?
A. The organization uses a decentralized privacy governance structure
B. The privacy program does not include a formal warning component
C. The organization doe* not have a dedicated privacy officer
D. Privacy policies ire only reviewed annually
Answer: A (LEAVE A REPLY)

NEW QUESTION: 304
When preparing a business case for the implementation of a security information and event management (SIEM) system, which of the following should be a PRIMARY driver in the feasibility study?
A. Implementation timeframe

B. Cost of software
C. Industry benchmarks
D. Cost-benefit analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 305
The MOST important outcome of information security governance is:
A. alignment with business goals.
B. informed decision making.
C. business risk avoidance
D. alignment with compliance requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 306
Which of the following BEST promotes stakeholder accountability in the management of information security risks?
A. Regular reviews for noncompliance
B. Establishment of information ownership
C. Targeted security procedures
D. Establishment of security baselines
Answer: B (LEAVE A REPLY)

NEW QUESTION: 307
Which of the following should be an information security manager's PRIMARY consideration when developing an incident response plan?
A. The organization's external communications plan
B. Skills and competencies of the help desk
C. The organization's risk tolerance and appetite
D. Incident response plan testing methods and frequency
Answer: D (LEAVE A REPLY)

NEW QUESTION: 308
For a user of commercial software downloaded from the Internet, which of the following is the MOST effective means of ensuring authenticity?
A. Digital signatures
B. Digital certificates
C. Digital code signing
D. Steganography
Answer: (SHOW ANSWER)

NEW QUESTION: 309

Who should decide the extent to which an organization will comply with new cybersecurity regulatory requirements?
A. IT steering committee
B. Senior management
C. Information security manager
D. Legal counsel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 310
Which of the following metrics is the MOST appropriate for measuring how well information security is performing in dealing with outside attacks?
A. Elapsed time to declare emergencies.
B. Elapsed time to resolve incidents
C. Number of incident detected.
D. Number of emergencies declared
Answer: B (LEAVE A REPLY)

NEW QUESTION: 311
Adding security requirements late in the software development life cycle (SDLC) would MOST likely result in:
A. clearer understanding of requirements.
B. operational efficiency.
C. cost savings.
D. compensating controls.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 312
Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?
A. Lack of visibility into previous data leakage incidents
B. An unusual upward trend in outbound email volume
C. Industry benchmark of DLP investments
D. A risk assessment on the threat of data leakage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 313
What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?
A. Benchmarking the expected value of the metrics against industry standards
B. Agreeing on baseline values for the metrics
C. Developing a dashboard for communicating the metrics

D. Providing real-time insight on the security posture of the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 314
When is the BEST time to identify the potential regulatory risk a new service provider presents to the organization?
A. During business case analysis
B. During contract negotiations
C. During due diligence
D. During integration planning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 315
Which of the following BEST determines an information asset's classification?
A. Directives from the data owner
B. Criticality to a business process
C. Value of the information asset to competitors
D. Cost of producing the information asset
Answer: (SHOW ANSWER)

NEW QUESTION: 316
Which of the following is the PRIMARY purpose for defining key performance indicators (KPIs) for a security program?
A. To measure the effectiveness of the security program
B. To ensure controls meet regulatory requirements
C. To evaluate the performance of security staff
D. To compare security program effectiveness to best practice
Answer: A (LEAVE A REPLY)

NEW QUESTION: 317
Which of the following is the MAIN objective of classifying a security incident as soon as it is discovered?

A. Downgrading the impact of the incident
B. Enabling appropriate incident investigation
C. Engaging appropriate resources
D. Preserving relevant evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 318
An information security manager has been informed of a new vulnerability in an online banking application, and a patch to resolve this issue is expected to be released in the next 72 hours. The information security manager s MOST important course of action is to:
A. run the application system m offline mode.
B. assess the risk and advise senior management
C. perform a business impact analysis (BIA).
D. identify and implement mitigating controls.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 319
Which of the following provides the GREATEST assurance that existing controls meet compliance requirements?
A. Performing a risk assessment
B. Evaluating metrics
C. Reviewing policies
D. Performing independent tests
Answer: B (LEAVE A REPLY)

NEW QUESTION: 320
A recent audit has identified that security controls required by the organization's policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?
A. Discuss the issue with data custodians to determine the reason for the exception.
B. Report the issue to senior management and request funding to fix the issue
C. Discuss the issue with data owners to determine the reason for the exception.
D. Deny access to the application until the issue is resolved.
Answer: (SHOW ANSWER)

NEW QUESTION: 321
Which of the following would BEST enable an organization to effectively monitor the implementation of standardized configurations?
A. Develop policies requiring use of the established benchmarks.
B. Implement a separate change tracking system to record changes to configurations.
C. Perform periodic audits to detect non-com pliant configurations.

D. Implement automated scanning against the established benchmarks.
Answer: (SHOW ANSWER)

NEW QUESTION: 322
Which of the following would BEST enable integration of information security governance into corporate governance?
A. Implementing IT governance, risk and compliance (IT GRC) dashboards
B. Having the CIO chair the information security steering committee
C. Using a balanced scorecard to measure the performance of the information security strategy
D. Ensuring appropriate business representation on the information security steering committee
Answer: C (LEAVE A REPLY)

NEW QUESTION: 323
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: 324
Which of the following incident response team (IRT) models is ideal for an organization that is regionally managed'
A. Coordinating IRT
B. Geographical IRT
C. Distributed IRT
D. Central IRT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 325
The GREATEST benefit of choosing a private cloud over a public cloud would be:
A. server protection.
B. collection of data forensic
C. online service availability.
D. containment of customer data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 326

A significant gap in an organization's breach containment process has been identified. Which of the following is MOST important for the information security manager to consider updating?
A. Incident test plan
B. Crisis management plan
C. Business continuity plan (BCP)
D. Incident response plan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 327
Planning for the implementation of an information security program is MOST effective when it:
A. applies gap analysts to current and future business plans
B. uses decision trees to prioritize security projects
C. uses risk-based analysis for security projects.
D. applies techno logy-driven solutions to Identified needs.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 328
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. Duplicate roles and responsibilities
C. Insufficient authority to perform duties effectively
D. Inadequate IT security controls to protect FT assets
Answer: A (LEAVE A REPLY)

NEW QUESTION: 329
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. Undefined thresholds to trigger alerts
B. Use of qualitative measures
C. Lack of formal KRI approval from IT management
D. Multiple KRIs for a single control process
Answer: (SHOW ANSWER)

NEW QUESTION: 330
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 alternative software solutions.
B. Assess the risk and impact to the business.
C. Segment the affected system on the network.
D. Research compensating security controls.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 331
Which of the following is the GREATEST risk to consider when a rival organization purchases a business unit within an organization?
A. Senior business management will not understand technical risks.
B. The business unit's confidential information will be transferred to the rival organization during the separation.
C. Access and permissions to the corporate network from the business unit will remain after the sale.
D. Loss of corporate knowledge.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 332
Which of the following is MOST critical for prioritizing actions in a business continuity plan (BCP)?
A. Risk assessment
B. Business process mapping
C. Business impact analysis (BIA)
D. Asset classification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 333
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. Review the providers serf-assessment
B. Check references supplied by the provider's other customers

C. Review the provider s information security policy.
D. Invoke the right to audit per the contract
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
Information security can BEST be enforced by making security:
A. a flexible system of procedures and guidelines.
B. a part of each employee's Job objectives.
C. a business process owner activity.
D. an integral component of corporate policies.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 335
Business applications should be selected for disaster recovery testing on the basis of:
A. recovery time objectives (RTOs).
B. the results of contingency desktop checks.
C. the number of failure points that are being tested.
D. criticality to the enterprise.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 336
An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST"
A. Application owners
B. Data owners
C. Communications department
D. Security operations team
Answer: D (LEAVE A REPLY)

NEW QUESTION: 337
An information security manager learns of a new international standard related to information security. Which of the following would be the BEST course of action?
A. Perform a gap analysis between the new standard and existing practices.
B. Consult with legal counsel on the standard's applicability to regulations
C. Determine whether the organization can benefit from adopting the new standard.
D. Review industry peers responses to the new standard.
Answer: (SHOW ANSWER)

NEW QUESTION: 338
After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?

A. Balanced scorecard
B. Recent audit results
C. Risk heat map
D. Gap analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 339
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. Encrypting the hard drive
C. Providing end-user awareness training focused on traveling with laptops
D. Deploying end-point data loss prevention software on the laptop
Answer: B (LEAVE A REPLY)

NEW QUESTION: 340
Which of the following should be the MOST important criteria when defining data retention policies?
A. Audit findings
B. Regulatory requirements
C. Industry best practices
D. Capacity requirements
Answer: B (LEAVE A REPLY)

NEW QUESTION: 341
Inadvertent disclosure of internal business information on social media is BEST minimized by which of the following?
A. Implementing data loss prevention (DLP) solutions
B. Limiting access to social media sites
C. Educating users on social media risks
D. Developing social media guidelines
Answer: D (LEAVE A REPLY)

NEW QUESTION: 342
What should be the PRIMARY basis for defining the appropriate level of access control to information assets?
A. Management requests
B. Audit findings
C. Compensating controls
D. Business needs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 343
Which of the following defines the MOST comprehensive set of security requirements for a newly developed information system?
A. Risk assessment results
B. Baseline controls
C. Key risk indicators (KRIs)
D. Audit findings
Answer: A (LEAVE A REPLY)

NEW QUESTION: 344
Which of the following is MOST helpful to an information security manager when determining service level requirements for an outsourced application?
A. Data classification
B. Information security policy
C. Application capabilities
D. Business functionality
Answer: A (LEAVE A REPLY)

NEW QUESTION: 345
Which of the following is the GREATEST risk associated with the installation of an intrusion prevention system (IPS)?
A. IPS logfiles may become too large to process.
B. Staff may not be able to access the Internet.
C. Critical business processes may be blocked.
D. Data links can no longer be encrypted end-to-end.
Answer: (SHOW ANSWER)

NEW QUESTION: 346
An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:
A. prepare properly vetted notifications regarding the incidents to external parties
B. document and report the root cause of the incidents for senior management
C. identify who should be held accountable for the security incidents.
D. identify security program gaps or systemic weaknesses that need correction.
Answer: (SHOW ANSWER)

NEW QUESTION: 347
When an operating system is being hardened, it is MOST important for an information security manager to ensure that
A. anonymous access is removed.
B. file access is restricted
C. default passwords are changed.
D. system logs are activated.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 348
Which of the following is the BEST course of action for an information security manager to align security and business goals?
A. Defining key performance indicators (KPIs)
B. Reviewing the business strategy
C. Conducting a business impact analysis (6IAJ
D. Actively engaging with stakeholders
Answer: (SHOW ANSWER)

NEW QUESTION: 349
The PRIMARY objective of periodically testing an incident response plan should be to:
A. improve internal processes and procedures,
B. highlight the importance of incident response and recovery.
C. improve employee awareness of the incident response process,
D. harden the technical infrastructure.
Answer: (SHOW ANSWER)

NEW QUESTION: 350
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. Communicate disciplinary procedures.
B. Define communication processes
C. Conduct incident response plan testing.

D. Document the incident response plan
Answer: (SHOW ANSWER)

NEW QUESTION: 351
In addition to business alignment and security ownership, which of the following is MOST critical for information security governance?
A. Executive sponsorship
B. Auditability of systems
C. Reporting of security metrics
D. Compliance with policies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 352
Which of the following is the MOST effective control to reduce the impact of ransomware attacks?
A. Backup strategy
B. Antivirus software
C. Security awareness training
D. Intrusion detection system (IDS)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 353
Which of the following BIST validates that security controls are implemented in a new business process?
A. Review the process for conformance with information security best practices
B. Benchmark the process against industry practices
C. Assess the process according to information security policy
D. Verify the use of a recognized control framework
Answer: (SHOW ANSWER)

NEW QUESTION: 354
Which of the following should be an information security manager's PRIMARY role when an organization initiates a data classification process?
A. Assign the asset classification level.
B. Verify that assets have been appropriately classified.
C. Define the classification structure to be implemented.
D. Apply security in accordance with specific classification.
Answer: (SHOW ANSWER)

NEW QUESTION: 355

Which of the following should an information security manager do FIRST after learning about a new regulation that affects the organization?

A. Notify the affected business units.

B. Assess the noncompliance risk.

C. Inform senior management of the new regulation.

D. Evaluate the changes with legal counsel.

Answer: (SHOW ANSWER)

NEW QUESTION: 356

The MOST important reason to maintain metrics for incident response activities is to

A. prevent incidents from reoccurring.

B. ensure that evidence collection and preservation are standardized

C. analyze security incident bends

D. support continual process improvement.

Answer: (SHOW ANSWER)

NEW QUESTION: 357

Which of the following factors is MOST likely to increase the chances of a successful social engineering attack?

A. Knowledge of internal procedures

B. Potential financial gain

C. Technical skills

D. Weak authentication for remote access

Answer: A (LEAVE A REPLY)

NEW QUESTION: 358

Which of the following is the MOST effective way to achieve the integration of information security governance into corporate governance?

A. Align information security budget requests to organizational goals.

B. Ensure information security efforts support business goals

C. Provide periodic IT balanced scorecards to senior management.

D. Ensure information security aligns with IT strategy.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 359

The MOST effective control to detect fraud inside an organization's network is to:

A. implement C (IDS).

B. segregate duties

C. review access logs.

D. apply two-factor authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 360
Which of the following is the MOST important requirement for the successful implementation of security governance?
A. Aligning to an international security framework
B. Implementing a security balanced scorecard
C. Performance an enterprise-wide risk assessment
D. Mapping to organizational
Answer: D (LEAVE A REPLY)

NEW QUESTION: 361
Which of the following is the MOST effective approach for integrating security into application development?
A. Defining security requirements
B. Including security in user acceptance testing sign-off
C. Performing vulnerability scans
D. Developing security models in parallel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 362
A validated patch to address a new vulnerability that may affect a mission-critical server has been released. What should be done immediately?
A. Conduct an impact analysis.
B. Take the server off-line and install the patch.
C. Add mitigating controls.
D. Check the server s security and install the patch.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 363
When implementing a new risk assessment methodology, which of the following is the MOST important requirement?
A. The methodology used must be consistent across the organization.

B. Risk assessments must be conducted by certified staff.
C. Risk assessments must be reviewed annually.
D. The methodology must be approved by the chief executive officer.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 364
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. determine daily downtime cost.
C. conduct a risk assessment
D. analyze cost metrics
Answer: B (LEAVE A REPLY)

NEW QUESTION: 365
Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?
A. Corresponding breaches associated with each vendor
B. Compliance requirements associated with the regulation
C. Compensating controls in place to protect information security
D. Criticality of the service to the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 366
An organization's information security manager will find it MOST difficult to perform a post-incident review of a data leakage event when it is related to:
A. private cloud services.
B. public cloud services
C. corporate mobile devices,
D. outsourced service providers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 367
It is suspected that key emails have been viewed by unauthorized parties. The email administrator conducted an investigation but it has not returned any information relating to the incident, and leaks are continuing. Which of the following is the BEST recommended course of action to senior management?
A. Commence security training for staff at the organization.
B. Rebuild the email application
C. Arrange for an independent review.

D. Restrict the distribution of confidential emails.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 368
Which of the following is MOST important to consider when developing a security awareness program in an organization?
A. Industry benchmarks
B. Established key risk indicators (KRIs)
C. Targeted monthly deliverables
D. Target audience demographics
Answer: (SHOW ANSWER)

NEW QUESTION: 369
Which is the BEST way for an organization to monitor security risk?
A. Analyzing key risk indicators (KRIs)
B. Analyzing key performance indicators (KPIs)
C. Using a dashboard to assess vulnerabilities
D. Using external risk intelligence services
Answer: (SHOW ANSWER)

NEW QUESTION: 370
To prevent computers on the corporate network from being used as part of a distributed denial of service (DDoS) attack, the information security manager should use:
A. incoming traffic filtering.
B. IT security policy dissemination.
C. rate limiting.
D. outgoing traffic filtering.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 371
When evaluating vendors for sensitive data processing, which of the following should be the FIRST step to ensure the correct level of information security is provided?
A. Review third-party reports of potential vendors.
B. Include information security criteria as part of vendor selection.
C. Include information security clauses in the vendor contract.
D. Develop metrics for vendor performance.
Answer: (SHOW ANSWER)

NEW QUESTION: 372
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. Isolate the server from the network.
B. Train the customer service team on properly controlling file permissions.
C. Report The situation to the data owner.
D. Remove access privileges to the folder containing the data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 373
Which of the following metrics would provide management with the MOST useful information about the effectiveness of a security awareness program?
A. Decreased number of phishing attacks
B. Increased number of reported security incidents
C. Decreased number of security incidents
D. Increased number of downloads of the organization's security policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 374
Which of the following is an organization's BEST approach for media communications when experiencing a disaster?
A. Defer public comment until partial recovery has been achieved.
B. Report high-level details of the losses and recovery strategy to the media.
C. Authorize a qualified representative to convey specially drafted messages.
D. Hold a press conference and advise the media to refer to legal authorities.
Answer: (SHOW ANSWER)

NEW QUESTION: 375
Which of the following is the BEST way to facilitate the alignment between an organization's information security program and business objectives?
A. The chief executive officer reviews and approves the information security program.
B. The information security program is audited by the internal audit department
C. The information security governance committee includes representation from key business areas.
D. Information security is considered at the feasibility stage of all I Perform a business impact analysisT projects
Answer: C (LEAVE A REPLY)

NEW QUESTION: 376
An information security manager has identified the organization is not in compliance with new legislation that will soon be in effect. Which of the following is MOST important to consider when determining additional controls to be implemented?

A. The organization's cost of noncompliance
B. The organization's risk appetite
C. The information security strategy
D. The information security policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 377
Which of the following should be the MOST important consideration when reporting sensitive risk-related information to stakeholders?
A. Transmitting the internal communication securely
B. Customizing the communication to the audience
C. Consulting with the public relations director
D. Ensuring nonrepudiation of communication
Answer: (SHOW ANSWER)

NEW QUESTION: 378
Which of the following would contribute MOST to employees' understanding of data handling responsibilities?
A. Implementing a tailored security awareness training program
B. Requiring staff acknowledgement of security policies
C. Demonstrating support by senior management of the security program
D. Labeling documents according to appropriate security classification
Answer: A (LEAVE A REPLY)

NEW QUESTION: 379
A new key business application has gone to production. What is the Most important reason to classify and determine the sensitivity of the data used by this application?
A. To minimize the cost of controls.
B. To ensure countermeasures are proportional to risk
C. To update the business impact analysis (BIA)
D. To determine retention requirements
Answer: B (LEAVE A REPLY)

NEW QUESTION: 380
The success of a computer forensic investigation depends on the concept of:
A. chain of evidence.
B. chain of attack.
C. evidence of attack.
D. forensic chain
Answer: A (LEAVE A REPLY)

NEW QUESTION: 381
Which of the following is the BEST indication that an organization is able to comply with information security requirements?
A. Maturity assessments have been performed for key business processes.
B. Senior management has approved the information security strategy.
C. Internal audit has not identified significant information security findings
D. Information security is included in business processes
Answer: (SHOW ANSWER)

NEW QUESTION: 382
Which of the following is MOST important for an information security manager to consider when developing a new information security policy?
A. Alignment with industry standards
B. Organizational culture and complexity
C. Organizational goals and objectives
D. Information security budget allocation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 383
The MOST important objective of security awareness training for business staff is to:
A. reduce negative audit findings
B. increase compliance.
C. modify behavior
D. understand intrusion methods
Answer: C (LEAVE A REPLY)

NEW QUESTION: 384
A policy has been established requiting users to install mobile device management (MDM) software on their personal devices Which of the following would BEST mitigate the risk created by noncompliance with this policy?
A. Requiring users to sign off on terms and conditions
B. Disabling remote access from the mobile device

C. Issuing company-configured mobile devices
D. Issuing warnings and documenting noncompliance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 385
When developing a protection strategy for outsourcing applications, the information se<urity manager MUST ensure that:
A. escrow agreements are in place.
B. nondisclosure clauses are in the contract.
C. the responsibility for security is transferred in the service level agreement (SLA).
D. the security requirements are included in the service level agreement (SLA).
Answer: (SHOW ANSWER)

NEW QUESTION: 386
A new version of an information security regulation is published that requires an organization's compliance. The information security manager should FIRST
A. conduct a risk assessment to determine the risk of noncompliance.
B. conduct benchmarking against similar organizations.
C. perform a gap analysis against the new regulation.
D. perform an audit based on the new version of the regulation
Answer: (SHOW ANSWER)

NEW QUESTION: 387
Which of the following would provide the MOST useful input when creating an information security program?
A. Key risk indicators (KRIs)
B. Information security budget
C. Business case
D. Information security strategy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 388
An organization rolled out information security awareness training and wants to perform an end-ot-year assessment to determine the program's success. Which of the following would be the BEST indicator of the program's effectiveness?
A. An increase in the number of employees completing training in a timely manner
B. An increase in the number of security-related inquiries to the help desk
C. An increase in the number of security incidents throughout the organization
D. An increase in the number of positive comments in trainee feedback surveys
Answer: B (LEAVE A REPLY)

NEW QUESTION: 389
Which of the following would BEST help an information security manager prioritize remediation activities to meet regulatory requirements?
A. Cost of associated controls
B. Annual toss expectancy (ALE) of noncompliance
C. A capability maturity model matrix
D. Alignment with the IT strategy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 390
Which of the following is an important criterion for developing effective key risk indicators (KRIs) to monitor information security risk?
A. The indicator should possess a high correlation with a specific risk and be measured on a regular basis
B. The indicator should provide a retrospective view of risk impacts and be measured annually.
C. The indicator should align with key performance indicators (KPIs) and measure root causes of process performance issues.
D. The indicator should focus on IT and accurately represent risk variances.
Answer: (SHOW ANSWER)

NEW QUESTION: 391
A hash algorithm is used to:
A. provide data confidentiality.
B. encrypt sensitive data files
C. verify the integrity of data files
D. verify the validity of the data in an email message
Answer: C (LEAVE A REPLY)

NEW QUESTION: 392

An information security manager is preparing a presentation to obtain support for a security initative. Which of the following is the BEST way to obtain management's commitment for the initiative?
A. Provide an analysis of current risk exposures.
B. include industry benchmarking comparisons.
C. Provide the estimated return on investment (ROI)
D. Include historical data of reported incidents.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 393
When developing a new application, which of the following is the BEST approach to ensure compliance with security requirements?
A. Provide security training for developers.
B. Perform a security gap analysis.
C. Prepare detailed acceptance criteria
D. Adhere to change management processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 394
When monitoring the security of a web-based application, which of the following is MOST frequently reviewed?
A. Access logs
B. Access lists
C. Threat metrics
D. Audit reports
Answer: (SHOW ANSWER)

NEW QUESTION: 395
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 encryption for account logins.
B. Rotate account passwords regularly.
C. Create unique login credentials for each user.
D. Utilize multi-factor authentication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 396
In a large organization, which of the following is the BEST source for identifying ownership of a PC?
A. Asset management register

B. User ID register
C. Identity management system
D. Domain name server (DNS) records
Answer: A (LEAVE A REPLY)

NEW QUESTION: 397
Which of the following would be MOST helpful in gaining support for a business case for an information security initiative?
A. Emphasizing threats to the organization
B. Demonstrating organizational alignment
C. Presenting a solution comparison matrix
D. Referencing control deficiencies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 398
An information security manager wants to document requirements detailing the minimum security controls required for user workstations. Which of the following resources would be MOST appropriate for this purpose?
A. Standards
B. Procedures
C. Guidelines
D. Policies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 399
A company has purchased a rival organization and is looking to integrate security strategies. Which of the following is the GREATEST issue to consider?
A. Differing security technologies
B. Differing security skills within the organizations
C. Confidential information could be leaked
D. The organizations have different risk appetites
Answer: A (LEAVE A REPLY)