ISACA.CISM.v2021-09-25.q217

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	217
Version:	v2021-09-25
# of views:	1843
# of Questions views:	81339
https://www.freecram.net/torrent/ISACA.CISM.v2021-09-25.q217.html	

NEW QUESTION: 1
Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?
A. Review the mitigating security controls
B. Assess the risk to the organization
C. Notify staff members of the threat
D. Increase the frequency of system backups
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
When selecting metrics to monitor the risks associated with an information security program, it is MOST important for an information security manager to:
A. consider the organization's business strategy.
B. identify the program's risk and compensating controls.
C. leverage industry benchmarks.
D. consider the strategic objectives of the program
Answer: (SHOW ANSWER)

NEW QUESTION: 3
What would be an information security manager's BEST recommendation upon learning that an existing contract with a third party does not clearly identify requirements for safeguarding the organization's critical data?
A. Cancel the outsourcing contract.
B. Initiate an external audit of the provider's data center.
C. Transfer the risk to the provider.
D. Create an addendum to the existing contract.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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. Reviewing each system's key performance indicators (KPIs)
B. Comparing the recovery point objectives (RPOs)
C. Evaluating the cost associated with each system's outage
D. Reviewing the business plans of each department
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following is the MOST likely outcome from the implementation of a security governance framework?
A. Increased availability of information systems
B. Realized business value from information security initiatives
C. Compliance with international standards
D. Cost reduction of information security initiatives
Answer: (SHOW ANSWER)

NEW QUESTION: 6
The PRIMARY reason to classify information assets should be to ensure
A. proper access control
B. senior management buy-in
C. proper ownership is established
D. Insurance valuation is appropriate.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following is the GREATEST benefit of integrating a security information and event management (SIEM) solution with traditional security tools such as IDS, anti-malware. and email screening solutions?
A. An increase in visibility into patterns of potential threats
B. The elimination of false positive detections
C. A reduction in operational costs
D. The consolidation of tools into a single console
Answer: (SHOW ANSWER)

NEW QUESTION: 8

After isolating a system compromised in a security incident, which of the following should be the PRIMARY objective of the information security team?

A. Providing response actions to restore the compromised system

B. Identifying the type of threat that compromised the system

C. Preserving the integrity of incident-related data

D. Implementing improvements to prevent recurrence of the incident

Answer: (SHOW ANSWER)

NEW QUESTION: 9

An organization has acquired a new system with strict maintenance instructions and schedules. Where should this information be documented?

A. Guidelines

B. Standards

C. Procedures

D. Policies

Answer: (SHOW ANSWER)

NEW QUESTION: 10

An information security manager is concerned about the risk of fire at its data processing center To address this concern, an automatic fire suppression system has been installed Which of the following risk treatments has been applied?

A. Mitigation

B. Transfer

C. Avoidance

D. Acceptance

Answer: A (LEAVE A REPLY)

NEW QUESTION: 11

An information security manager recently received funding for a vulnerability scanning tool to replace manual assessment techniques and needs to justify the expense of the tool going forward. Which of the following metrics would BEST indicate the tool is effective?

A. A decrease in the lime needed to detect vulnerabilities

B. An increase in the number of detected vulnerabilities

C. A decrease in staff needed to detect vulnerabilities

D. An increase in the severity of detected vulnerabilities

Answer: (SHOW ANSWER)

NEW QUESTION: 12

For an organization that provides web-based services, which of the following security events would MOST likely initiate an incident response plan and be escalated to management?

A. Suspicious network traffic originating from the demilitarized zone (DMZ)

B. Several port scans of the web server
C. Multiple failed login attempts on an employee's workstation
D. Anti-malware alerts on several employees' workstations
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following should cause the GREATEST concern for an information security manager reviewing the effectiveness of an intrusion prevention system (IDS)?
A. Increase in false negatives
B. Increase in crossover error rate
C. Decrease in false positives
D. Decrease in malicious packets
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which of the following is the GREATEST risk associated with the installation of an intrusion prevention system (IPS)?
A. Staff may not be able to access the Internet.
B. Data links can no longer be encrypted end-to-end.
C. Critical business processes may be blocked.
D. IPS logfiles may become too large to process.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following provides the GREATEST assurance that information security is addressed in change management?
A. Reviewing changes from a security perspective
B. Requiring senior management sign-off on change management
C. Providing security training for change advisory board
D. Performing a security audit on changes
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following BEST demonstrates return on investment (ROI) for an information security initiative?
A. Risk heat map
B. Business impact analysis (BIA)
C. Business case
D. Information security program roadmap
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following types of controls would be MOST important to implement when digitizing human resource (HR) records?
A. Software development controls
B. Access management controls
C. Project management controls
D. Change management controls
Answer: (SHOW ANSWER)

NEW QUESTION: 18
What is the GREATEST benefit of classifying assets based on sensitivity?
A. The organization can allocate appropriate levels of protection.
B. Data is available to appropriately assign asset ownership.
C. Staff can create more realistic risk scenarios.
D. The organization is in compliance with regulatory guidelines.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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. Research mobile device management (MDM) solutions.
B. Assess risks introduced by the technology
C. Conduct a vulnerability assessment on the devices.
D. Develop an acceptable use policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following processes BEST supports the evaluation of incident response effectiveness?
A. Incident logging
B. Chain of custody
C. Root cause analysis
D. Postincident review

Answer: (SHOW ANSWER)

NEW QUESTION: 21
An organization wants to enable digital forensics for a business-critical application. Which of the following will BEST help to support this objective?
A. Develop an incident response plan.
B. Define data retention criteria.
C. Install biometric access control.
D. Enable activity logging.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
The Information security manager and senior management of a global financial institution have been notified of a potential breach to its database containing a large volume of sensitive information Which of the following should be done FIRST?
A. Isolate the breached database.
B. Notify law enforcement
C. Assess the possible impact
D. Implement mitigating controls.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23
Which of the following is the MOST reliable way to ensure network security incidents are Identified as soon as possible'
A. Tram help desk staff to identify and prioritize security incidents
B. Collect and correlate IT Infrastructure event logs
C. Conduct workshops and training sessions with end users.
D. Install stateful inspection firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 24
The responsibility for approving access to data according to the organization's data classification policy belongs to the:
A. data end user
B. information security manager
C. system administrator.
D. data owner
Answer: (SHOW ANSWER)

NEW QUESTION: 25

Which of the following is the MOST important consideration when selecting members for an information security steering committee?
A. Information security expertise
B. Tenure in the organization
C. Cross-functional composition
D. Business expertise
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What information is MOST helpful in demonstrating to senior management how information security governance aligns with business objectives?
A. Metrics of key information security deliverables
B. Drafts of proposed policy changes
C. Updates on information security projects in development
D. A list of monitored threats, risks and exposures
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which of the following will BEST enable the identification of appropriate controls to prevent repeated occurrences of similar types of information.....
A. Perform a root cause analysis of the security incidents.
B. Review existing preventive controls for security weaknesses.
C. Review lessons learned with key stakeholders.
D. Perform a business impact analysis (BIA) of the security incidents.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following metrics would BEST monitor how well information security requirements are incorporated into the change management process?
A. Denied changes due to insufficient security details
B. Information security related changes
C. Unauthorized changes in the environment
D. Information security incidents caused due to unauthorized changes
Answer: (SHOW ANSWER)

NEW QUESTION: 29
An organization has decided to implement a security information and event management (SIEM) system. It is MOST important for the organization to consider:
A. log sources.
B. data ownership.
C. threat assessments.

D. industry best practices.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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. Provide yearly competitive pricing to illustrate the value of the IPS.
B. Establish and present appropriate metrics that track performance
C. Perform industry research annually and document the overall ranking of the IPS
D. Perform a penetration test to demonstrate the ability to protect
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following is the MOST important consideration during a forensics investigation?
A. Evidence hardening
B. Disclosure requirements
C. Chain of custody
D. Management directives
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following is MOST important for the alignment of an information security program with the information security strategy?
A. Adoption of an industry recognized framework
B. Input from senior management
C. Benchmarking against industry peers
D. Identification of business-specific risk factors
Answer: (SHOW ANSWER)

NEW QUESTION: 33

Senior management is alarmed by recent media reports of severe security incidents at competing organizations Which of the following would provide the BEST assurance that the organization's current security measures are performing adequately?

A. Require third-party penetration testing

B. Review the intrusion detection system (IDS) logs

C. Review the intrusion prevention system (IPS) logs

D. Require internal penetration testing

Answer: (SHOW ANSWER)

NEW QUESTION: 34

What is the PRIMARY benefit of effective configuration management?

A. Decreased risk to the organization's systems

B. Reduced frequency of incidents

C. Standardization of system support

D. Improved vulnerability management

Answer: (SHOW ANSWER)

NEW QUESTION: 35

Which of the following should be done FIRST when implementing an information security strategy?

A. Determine the desired state of information security.

B. Identify owners of information assets

C. Map business goals to information security strategy objectives.

D. Benchmark the strategy with industry peers.

Answer: (SHOW ANSWER)

NEW QUESTION: 36

Which of the following is the MOST important reason to have documented security procedures and guidelines?

A. To allocate security responsibilities to staff

B. To meet regulatory compliance requirements

C. To enable standard security practices

D. To facilitate collection of security metrics

Answer: (SHOW ANSWER)

NEW QUESTION: 37

Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Base mandatory review and exception approvals on residual risk.

B. Require users to acknowledge the acceptable use policy.

C. Base mandatory review and exception approvals on inherent risk.

D. Require the steering committee to review exception requests
Answer: (SHOW ANSWER)

NEW QUESTION: 38
What is the BEST way to determine the level of risk associated with information assets processed by an IT application?
A. Research compliance requirements associated with the information.
B. Calculate the business value of the information assets.
C. Review the cost of acquiring the information assets for the business.
D. Evaluate the potential value of information for an attacker.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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. Report the results of a security control self-assessment (CSA).
B. Benchmark security metrics against industry standard
C. Present a penetration testing report conducted by a third party
D. Provide a summary of security project return on investments (ROIs) for the past year.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
A validated patch to address a new vulnerability that may affect a mission-critical server has been released.
What should be done immediately?

A. Check the server s security and install the patch.
B. Take the server off-line and install the patch.
C. Conduct an impact analysis.
D. Add mitigating controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following is MOST important lo track for determining the effectiveness of an information security program?
A. Service level agreements (SLAs)
B. Key performance indicators (KPIs)
C. Return on investment (ROI)
D. Key risk indicators (KRIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 42

Which of the following should an information security manager consider when reviewing an existing security investment plan?
A. The plan focuses on meeting industry best practices and industry standards.
B. The plan has summarized IT costs for implementation.
C. The plan is based on a review of threats. and vulnerabilities in existing IT systems.
D. The plan identifies all potential threats and their impact on business processes
Answer: (SHOW ANSWER)

NEW QUESTION: 43
When monitoring the security of a web-based application, which of the following is MOST frequently reviewed?
A. Audit reports
B. Access lists
C. Access logs
D. Threat metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 44
What is the FIRST line of defense against criminal insider activities?
A. Validating the integrity of personnel
B. Signing security agreements by critical personnel
C. Monitoring employee activities
D. Stringent and enforced access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 45
An information security manager has recently been notified of potential security risks associated with a thirdparty service provider. What should be done NEXT to address this concern?
A. Escalate to the chief risk officer
B. Conduct a vulnerability analysis
C. Determine compensating controls
D. Conduct a risk analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 46
A business manager has decided not to implement a control based on the risk assessment of a mission-critical business application because of its impact on performance. What is the information security manager's BEST course of action'?
A. Escalate the issue to senior management for a final decision.
B. Instruct the business manager to implement the mitigation control.
C. Recommend possible compensating controls.

D. Update the organization's risk profile.
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which of the following is the BEST evidence of an effectively designed key risk indicator (KRI)?
A. The KRI predicts threats
B. The KRI measures inherent risk.
C. The KRI is quantitative
D. The KRI incorporates risk appetite
Answer: (SHOW ANSWER)

NEW QUESTION: 48
A company is considering a new automated system that requires implementation of wireless devices for data capture. Even though wireless is not an approved technology, senior management has accepted the risk and approved a Proof-of-Concept (POC) to evaluate the technology and proposed solution. Which of the following is the information security manager s BEST course of action?
A. Implement a wireless intrusion detection system (IDS).
B. Develop corporate wireless standards.
C. Provide personnel with wireless security training.
D. Sandbox the proposed solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
To help users apply appropriate controls related to data privacy regulation, what is MOST important to communicate to the users?
A. Data storage procedures
B. Results of penetration testing
C. Data classification policy
D. Features of data protection products
Answer: (SHOW ANSWER)

NEW QUESTION: 50

Which of the following is the MAIN reason for integrating an organization's incident response plan with its business continuity process?

A. Recovery time objectives (RTOs) need to be determined.

B. Incidents can escalate into disasters needing proper response

C. Integration of the plan will reduce resource costs to the organization.

D. Incidents will be reported more timely when categorized as a disaster.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

Which of the following is the GREATEST benefit of a centralized approach to coordinating information security?

A. Optimal use of security resources

B. Business user buy-in

C. Integration with business functions

D. Reduction in the number of policies

Answer: (SHOW ANSWER)

NEW QUESTION: 52

Which of the following provides the MOST essential input for the development of an information security strategy?

A. Measurement of security performance against IT goals

B. Results of an information security gap analysis

C. Results of a technology risk assessment

D. Availability of capable information security resources

Answer: (SHOW ANSWER)

NEW QUESTION: 53

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. Escalate the noncompliance issues to senior management

B. Develop a solution independently

C. Perform a risk assessment.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 54

Which of the following is MOST helpful to developing a comprehensive Information security strategy?

A. Conducting a risk assessment

B. Performing a business impact analysts (BIA).

C. Gathering business objectives
D. Adopting an industry framework
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following is the BEST option for addressing regulations that will adversely affect the allocation of information security program resources?
A. Determine compliance levels of peer organizations.
B. Conduct assessments for management decisions.
C. Delay implementation of compliance activities.
D. Prioritize compliance efforts based on probability.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which of the following BEST demonstrates that the objectives of an information security governance framework are being met?
A. Balanced scorecard
B. Key performance indicators (KPIs)
C. Penetration test results
D. Risk dashboard
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which of the following would BEST enable an effective response to a network-based attack?
A. Maintaining an incident playbook
B. Deploying counterattacks on the source network
C. Notifying the network service provider of incidents
D. Enabling network time protocol synchronization
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which of the following is the BEST way to ensure that organizational security policies comply with data security regulatory requirements?
A. Send the policies to stakeholders for review
B. Align the policies to the most stringent global regulations.
C. Obtain annual sign-off from executive management.
D. Outsource compliance activities
Answer: (SHOW ANSWER)

NEW QUESTION: 59

An organization must meet rigorous breach reporting standards in order to comply with regulatory requirements. Which of the following is the BEST way to minimize the organization's financial exposure if a service provider experiences a breach?

A. Include the reporting requirements in the provider contract.

B. Require the provider to comply with organization's information security policy.

C. Review the reporting requirements and processes contained in the provider's policies.

D. Verify the provider has automated reporting processes in place.

Answer: (SHOW ANSWER)

NEW QUESTION: 60

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

A. Document and schedule a date to revisit the issue.

B. Shut down the business application.

C. Determine a lower-cost approach to remediation.

D. Document and escalate to senior management.

Answer: (SHOW ANSWER)

NEW QUESTION: 61

Which of the following is the MOST important consideration to provide meaningful information security reporting to senior management?

A. Communicating risk in financial terms

B. Compliance with industry best practice

C. Benchmarking against industry peers

D. Mapping to business initiatives

Answer: (SHOW ANSWER)

NEW QUESTION: 62

In a large organization requesting outsourced services, which of the following contract clauses is MOST important to the information security manager?

A. Nondisclosure clause

B. Frequency of status reporting
C. Compliance with security requirements
D. Intellectual property
Answer: (SHOW ANSWER)

NEW QUESTION: 63
The business advantage of implementing authentication tokens is that they:
A. provide nonrepudiation
B. reduce overall cost
C. improve access security
D. reduce administrative workload
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?
A. Integrating the risk assessment into the internal audit program
B. Applying global security standards to the IT projects
C. Having the information security manager participate on the project steering committees
D. Training project managers on risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 65
A recent comprehensive vulnerability assessment identified emerging threats to the continuity of critical business services. What should be the information security manager s FIRST course of action?
A. Conduct a risk assessment.
B. Perform a penetration test.
C. Perform a patch update.
D. Conduct a gap analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following is the GREATEST concern with employees investigating and responding to security breaches they report'?
A. Loss of confidential information
B. Evidence contamination
C. Segregation of duty violations
D. Loss of business productivity
Answer: (SHOW ANSWER)

NEW QUESTION: 67
An organization has acquired a company in a foreign country to gain an advantage in a new market Which of the following is the FIRST step the information security manager should take?
A. Merge the two existing information security programs
B. Apply the existing information security program to the acquired company
C. Evaluate the information security laws that apply to the acquired company
D. Determine which country's information security regulations will be used
Answer: (SHOW ANSWER)

NEW QUESTION: 68
When designing security controls, it is MOST important to:
A. evaluate the costs associated with the controls.
B. apply a risk-based approach.
C. apply controls to confidential information.
D. focus on preventive controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
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 ensure that the mitigation effort does not exceed the asset value
C. To ensure that benefits are aligned with business strategies
D. To justify information security program activities
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

A. Review and update existing security policies.
B. Enforce passwords and data encryption on the devices.
C. Conduct security awareness training.
D. Require remote wipe capabilities for devices.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
The BEST way to avoid session hijacking is to use:
A. a secure protocol.
B. a reverse lookup.
C. a firewall
D. strong password controls.

Answer: (SHOW ANSWER)

NEW QUESTION: 72
An organization is considering moving lo a cloud service provider for the storage of sensitive data Which of the following .... consideration FIRST?
A. Requirements for data encryption
B. Right to terminate clauses In the contract
C. Results of the cloud provider's control report
D. A destruction-of-data clause m the contract
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following is the MOST important factor to be considered when reviewing an information security strategy?
A. Benchmarking to industry peers
B. Unmitigated risk
C. Frequency of security incidents
D. Evolving business goals
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following is the BEST indicator that an organization is appropriately managing risk?
A. Risk assessment results are within tolerance
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. The number of security incident events reported by staff has increased
Answer: (SHOW ANSWER)

NEW QUESTION: 75
In which cloud model does the cloud service buyer assume the MOST security responsibility?
A. Platform as a Service (PaaS)
B. Infrastructure as a Service (laaS)
C. Disaster Recovery as a Service (DRaasS)
D. Software as a Service (SaaS)
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following would be MOST helpful to an information security manager tasked with enforcing enhanced password standards?
A. Implementing technical password controls to include strong complexity
B. Conducting password strength testing

C. Implementing a centralized identity management system
D. Reeducating end users on creating strong, complex passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which of the following BEST supports the alignment of information security with business functions?
A. Creation of a security steering committee
B. IT management support of security assessments
C. A focus on technology security risk within business processes
D. Business management participation in security penetration tests
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following is MOST important for an information security manager to ensure when evaluating change requests?
A. Contingency plans have been created.
B. Residual risk is within risk tolerance.
C. Requests are approved by process owners.
D. Requests add value to the business.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
An information security manager has been tasked with implementing a security awareness training program Which of this ..... have the MOST influence on the effectiveness of this program?
A. Obtaining buy-in from senior management
B. Tailoring the training to the organization's environment
C. Obtaining buy-in from end users
D. Basing the training program on industry best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 80

Which of the following is the MOST important consideration when updating procedures for managing security devices?

A. Updates based on changes in risk, technology, and process
B. Updates based on the organization's security framework
C. Review and approval of procedures by management
D. Notification to management of the procedural changes
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following is the BEST method to protect consumer private information for an online public website?
A. Use secure encrypted transport layer.
B. Encrypt consumer's data in transit and at rest.
C. Apply a masking policy to the consumer data.
D. Apply strong authentication to online accounts.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which of the following trends BEST indicates that the maturity level of an information security program is improving?
A. A decrease in residual risk
B. An increase in control self-assessments (CSAs) performed
C. An increase in overall security funding
D. A decrease in the number of security incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 83
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: 84
Which of the following is necessary to determine what would constitute a disaster for an organization?
A. Risk analysis
B. Threat probability analysis
C. Recovery strategy analysis

D. Backup strategy analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 85
To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:
A. assess the risks of all new equipment.
B. assess security during equipment deployment.
C. ensure compliance during user acceptance testing.
D. develop an approved equipment list.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which of the following reports would provide the BEST overview of the progress of an information security program to senior management?
A. Results of the last penetration test
B. Inventory of information technology security controls
C. Heat map of the current risk landscape
D. Key performance indicators (KPIs) related to security initiatives
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following provides the GREATEST assurance that existing controls meet compliance requirements?
A. Evaluating metrics
B. Reviewing policies
C. Performing independent tests
D. Performing a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following should be determined FIRST when preparing a risk communication plan?
A. Reporting content
B. Communication channel
C. Target audience
D. Reporting frequency
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Which of the following is MOST important when developing a security strategy?
A. Sufficient resource allocation by management

B. A risk-aware security culture
C. Management direction on security
D. A well-defined security organization
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Which of the following is the MOST important factor of a successful information security program?
A. The program is cost-efficient and within budget.
B. The program follows industry best practices
C. The program is focused on risk management.
D. The program is based on a well-developed strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following would provide the BEST evidence to senior management that security control performance has improved?
A. Reduction in inherent risk
B. Demonstrated return on security investment
C. Results of an emerging threat analysis
D. Review of security metrics trends
Answer: (SHOW ANSWER)

NEW QUESTION: 92
When creating a bring your own device (BYOD) program, it is MOST important to:
A. balance the costs between private versus business usage and define the method to track usage.
B. establish metrics to evaluate the effectiveness of the program.
C. develop remote wipe capabilities and procedures.
D. ensure the organization's ownership of data and management of the device.
Answer: (SHOW ANSWER)

NEW QUESTION: 93

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. Understanding of the current business strategy
D. Benchmarking against industry best practice
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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: (SHOW ANSWER)

NEW QUESTION: 95
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. perform an assessment to measure the current state
B. ensure baseline back-ups are performed.
C. inform senior management of changes in risk metrics.
D. deliver security awareness training.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
What should be the FIRST step when developing an asset management program?
A. Encrypt assets containing sensitive data.
B. Create an asset inventory.
C. Classify assets according to risk.
D. Create a configuration management database
Answer: (SHOW ANSWER)

NEW QUESTION: 97
An information security manager is planning to purchase a mobile device management (MDM) system to manage personal devices used by employees to access corpor Which of the following is MOST important to include in the business case?
A. Cost-benefit analysis
B. Identified risks and mitigating controls
C. Information security-related metrics
D. Industry best practice benchmarking results

Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following has the MOST influence on an organization's adoption of information security policies?
A. A comprehensive security awareness program
B. Established key performance indicators (KPIs)
C. Demonstrated senior management commitment
D. Enforcement of penalties for noncompliance
Answer: (SHOW ANSWER)

NEW QUESTION: 99
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. Request additional funding for recruiting and training
D. Benchmark to an industry peer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following is the PRIMARY objective of an incident response plan?
A. To minimize business disruption
B. To establish appropriate service level agreements (SLAs)
C. To define roles and responsibilities
D. To communicate escalation procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Which of the following would be MOST important to include in a bring your own device (BYOD) policy with regard to lost or stolen devices? The need for employees to:
A. request a remote wipe of the device
B. notify local law enforcement.
C. initiate the company's incident reporting process
D. seek advice from the mobile service provider
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following activities would BEST incorporate security into the software development life cycle
{SOLO7

A. Test applications before go-live
B. Scan operating systems for vulnerabilities
C. Include security training for the development team
D. Minimize the use of open source software
Answer: (SHOW ANSWER)

NEW QUESTION: 103
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: 104
An organization Is storing accounting data in an external cloud environment. Which of the following is the MOST important riskrelated consideration?
A. Access authorization to the data
B. Data backup capabilities
C. Access to physical servers hosting the data
D. Availability of audit logs
Answer: (SHOW ANSWER)

NEW QUESTION: 105
An incident response team has determined there is a need to isolate a system that is communicating with a known malicious host on the Internet, following stakeholders should be contacted FIRST?
A. The business owner
B. System administrator
C. Key customers
D. Executive management
Answer: (SHOW ANSWER)

NEW QUESTION: 106
When developing an incident response plan, the information security manager should:
A. allow IT to decide which systems can be removed from the infrastructure.
B. require IT to invoke the business continuity plan (BCP).
C. determine recovery time objectives (RTOs).
D. include response scenarios that have been approved previously by business management.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Segregation of duties is a security control PRIMARILY used to:
A. establish dual check.
B. establish hierarchy.
C. limit malicious behavior.
D. decentralize operations.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which of the following is the BEST course of action for an information security manager to align security and business goals?
A. Reviewing the business strategy
B. Defining key performance indicators (KPIs)
C. Conducting a business impact analysis (6IAJ
D. Actively engaging with stakeholders
Answer: (SHOW ANSWER)

NEW QUESTION: 109
An organization engages 4 third-party vendor to monitor and support a financial application under scrutiny by regulators. Maintaining strict data integrity and confidentiality for this application is critical to the business. Which of the following controls would MOST effectively manage risk to the organization?
A. Disabling vendor access and only re-enabling when access is needed
B. Activating access and data logging
C. Implementing segregation of duties between systems and data
D. Implementing periodic access reviews of vendor employees
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
The BEST way to report to the board on the effectiveness of the information security program is to present:

A. poor-group Industry benchmark.

B. a dashboard illustrating key performance metrics.
C. a report of cost savings from process improvements
D. a summary of the most recent audit findings.
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which of the following is the MOST effective way to mitigate the risk of confidential data leakage to unauthorized stakeholders?
A. Create a data classification policy.
B. Require the use of login credentials and passwords.
C. Conduct information security awareness training.
D. Implement role-based access controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Who should be responsible for determining the classification of data within a database used in conjunction with an enterprise application?
A. Database architect
B. Information security manager
C. Data owner
D. Database administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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. Incident classification
B. Forensic analysis
C. Incident response
D. Vulnerability assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 114
A core business unit relies on an effective legacy system that does not meet the current security standards and threatens that enterprise network. Which of the following is the BEST course of action to address the situation?
A. Develop processes to compensate for the deficiencies.
B. Disconnect the legacy system from the rest of the network.
C. Document the deficiencies in the risk register.
D. Require that new systems that can meet the standards be implemented.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
A regulatory organization sends an email to an information security manager warning of an Impending cyber attack. What should the information security manager do FIRST?
A. Validate the authenticity of the alert.
B. Determine whether the attack is in progress.
C. Alert the network operations center
D. Reply asking for more details.
Answer: (SHOW ANSWER)

NEW QUESTION: 116
The PRIMARY reason for defining the information security roles and responsibilities of staff throughout an organization is to:
A. enforce individual accountability.
B. reinforce the need for training.
C. increase corporate accountability
D. comply with security policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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. document the risk exception
B. review existing technical controls.
C. continue implementing the control.
D. recommend compensating controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 118
An information security manager has identified and implemented mitigating controls according to industry best practices. Which of the following is the GREATEST risk associated with this approach?
A. The cost of control implementation may be too high.
B. The security program may not be aligned with organizational objectives.
C. Important security controls may be missed without senior management input.
D. The mitigation measures may not be updated in a timely manner.
Answer: (SHOW ANSWER)

NEW QUESTION: 119

An organization's security was compromised by outside attackers. The organization believed that the incident was resolved. After a few days, the IT staff is still noticing unusual network traffic. Which of the following is the BEST course of action to address this situation?

A. Assess the level of the residual risk.

B. Identify potential incident impact.

C. Implement additional incident response monitoring tools.

D. Initiate the incident response process.

Answer: (SHOW ANSWER)

NEW QUESTION: 120

Which of the following would provide the MOST effective security outcome in an organization?

A. Extending security assessment to cover asset disposal on contract termination

B. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage

C. Extending security assessment to include random penetration testing

D. Ensuring security requirements are defined at the request-for-proposal (RFP) stage

Answer: (SHOW ANSWER)

NEW QUESTION: 121

Which of the following is the PRIMARY reason to include message templates for communications with external parties in an incident response plan?

A. To eliminate reliance on a communications specialist

B. To communicate efficiently and consistently

C. To automate communication with external parties without delay

D. To ensure that messages to external parties are complete and accurate

Answer: (SHOW ANSWER)

NEW QUESTION: 122

In the development of an information security strategy, recovery time objectives (RTOs) will serve as indicators of:

A. senior management support.

B. maturity levels.

C. open vulnerabilities.

D. risk tolerances.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
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. External audit results
C. Acceptable risk level
D. Annual loss expectancy
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which of the following is a potential indicator of inappropriate Internet use by staff?
A. Increased help desk calls for password resets
B. Increased reports of slow system performance
C. Increased number of weaknesses from vulnerability scans
D. Reduced number of pings on firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Who should have PRIMARY responsibility for authorizing access to data residing in an enterprise resource application?
A. Application administrator
B. Identity and access management team
C. Process owner
D. Data custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 126
Which of the following is the MOST significant security risk in IT asset management?
A. Unregistered IT assets may not be configured properly.
B. Unregistered IT assets may riot be included in security documentation.
C. IT assets may be used by staff for private purposes.
D. Unregistered IT assets may not be supported.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
An information security manager has researched several options for handling ongoing security concerns and will be presenting these solutions to business managers. Which of the following with BEST enable business managers to make an informed decision?

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

NEW QUESTION: 128
Which of the following is MOST important to the effectiveness of an information security steering committee?
A. The committee has strong representation from IT.
B. The committee is driven by industry best practices.
C. The committee has cross-organizational representation.
D. The committee has strong regulatory knowledge.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Which of the following should an information security manager perform FIRST when an organization's residual risk has increased?
A. Implement security measures to reduce the risk.
B. Assess the business impact.
C. Communicate the information to senior management.
D. Transfer the risk to third parties.
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following is the MOST effective way to help ensure information security programs are aligned with business objectives?

A. Develop information security policies based on laws and regulations.
B. Establish and monitor information security performance metrics for the business.
C. Include business unit representation in the information security steering committee.
D. Implement information security awareness campaigns for business units.
Answer: (SHOW ANSWER)

NEW QUESTION: 131
Management has expressed concerns to the information security manager that shadow IT may be a risk to the organization. What is the FIRST step the information security manager should take?
A. Update the security policy to address shadow IT.
B. Determine the value of shadow IT projects.
C. Determine the extent of shadow IT usage.
D. Block the end user's ability to use shadow IT

Answer: (SHOW ANSWER)

NEW QUESTION: 132
Which activity is MOST important when identifying the appropriate security controls for a new business application?
A. Interviewing senior management
B. Conducting a risk assessment
C. Performing a business impact analysts (BIA)
D. Assigning data classification to assets
Answer: (SHOW ANSWER)

NEW QUESTION: 133
What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?
A. Test incident response procedures regularly.
B. Establish and measure key performance indicators (KPIs)
C. Obtain senior management commitment
D. Communicate incident response procedures to staff.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 134
Risk identification, analysis, and mitigation activities can BCST be integrated into business life cycle processes by linking them to:
A. configuration management.
B. continuity planning
C. compliance testing
D. change management
Answer: (SHOW ANSWER)

NEW QUESTION: 135
After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?
A. Recent audit results
B. Balanced scorecard
C. Gap analysis
D. Risk heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 136
An organization is considering the deployment of encryption software and systems organization-wide. The MOST important consideration should be whether:

A. the implementation supports the business strategy.
B. a classification policy has been developed to incorporate the need for encryption,
C. data can be recovered if the encryption keys are misplaced
D. the business strategy includes exceptions to the encryption standard.
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which of the following is MOST relevant for an information security manager to communicate to IT operations?
A. The level of exposure
B. The level of inherent risk
C. Threat assessments
D. Vulnerability assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which of the following is MOST important to the successful development of an information security strategy?
A. Approved policies and standards
B. An implemented development life cycle process
C. A well-implemented governance framework
D. Current state and desired objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?
A. Develop the test plan.
B. Identify recovery time objectives (RTOs).
C. Define response team roles
D. Analyze the business impact.
Answer: (SHOW ANSWER)

NEW QUESTION: 140

Which of the following is MOST helpful in identifying external and internal factors that could influence the organization's future information security posture?

A. SWOT analysis

B. Current risk tolerance

C. Penetration testing

D. IT balanced scorecard

Answer: (SHOW ANSWER)

NEW QUESTION: 141

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 update the business impact analysis (BIA)

B. To minimize the cost of controls.

C. To determine retention requirements

D. To ensure countermeasures are proportional to risk

Answer: (SHOW ANSWER)

NEW QUESTION: 142

The PRIMARY purpose of establishing an information security governance framework should be to:

A. document and communicate how the information security program functions within the organization.

B. align information security strategy and investments to support organizational activities.

C. align corporate governance, activities, and investments to information security goals.

D. establish the business case for strategic integration of information security in organizational efforts.

Answer: (SHOW ANSWER)

NEW QUESTION: 143

Which of the following would BEST enable effective decision-making?

A. Formalized acceptance of risk analysis by business management

B. Annualized loss estimates determined from past security events

C. A universally applied list of generic threats, impacts, and vulnerabilities

D. A consistent process to analyze new and historical information risk

Answer: (SHOW ANSWER)

NEW QUESTION: 144

Which of the following is the MOST effective method of determining security priorities?

A. Vulnerability assessment

B. Impact analysis
C. Gap analysis
D. Threat assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 145
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. Application capabilities
C. Business functionality
D. Information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 146
An organization has announced company-wide budget cuts due to poor financial performance, impacting delivery of the information security program. What should the information security manager do FIRST?
A. Reduce the scope of existing security Initiatives to lower the total cost.
B. Inform senior management of the increased risk associated with lack of funding.
C. Prioritize projects within the information security program.
D. Reduce the number of Information security projects to adhere to the new budget.
Answer: (SHOW ANSWER)

NEW QUESTION: 147
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process Is to:
A. obtain the support of executive management.
B. identify critical processes and the degree of reliance on support services.
C. document the disaster recovery process.
D. map the business process to supporting IT and other corporate resources.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
In a multinational organization, local security regulations should be implemented over global security policy because:
A. global security policies include unnecessary controls for local businesses
B. business objectives are defined by local business unit managers.
C. deploying awareness of local regulations is more practical than of global policy.
D. requirements of local regulations take precedence
Answer: (SHOW ANSWER)

NEW QUESTION: 149
Which of the following is the BEST method to protect against data exposure when a mobile device is stolen?
A. Remote wipe capability
B. Encryption
C. Insurance
D. Password protection
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Which of the following should an information security manager do FIRST when a recent internal audit reveals a security risk is more severe than previously assessed?

A. Validate the finding is legitimate and not a false positive.
B. Review the remainder of the internal audit report.
C. Update the risk register and notify the CISC
D. Escalate the finding to the business owner and obtain a remediation plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 151
An organization has implemented a bring your own device (BYOD)} program. Which of the following is the GREATEST risk to the organization?
A. Device theft
B. Data leakage
C. Lack of nonrepudiation
D. Device incompatibility
Answer: (SHOW ANSWER)

NEW QUESTION: 152
During which stage of the software development life cycle (SDLC) should application security controls FIRST be addressed?
A. Application system design

B. Software code development
C. Requirements gathering
D. Configuration management
Answer: (SHOW ANSWER)

NEW QUESTION: 153
The PRIMARY reason for using information security metrics is to:
A. ensure alignment with corporate requirements.
B. achieve senior management commitment.
C. adhere to legal and regulatory requirements
D. monitor the effectiveness of controls
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which of the following is the MOST relevant risk factor to an organization when employees use social media?
A. Social media can be accessed from multiple locations.
B. Social media increases the velocity of risk and the threat capacity.
C. Social media offers a platform that can host cyber-attacks.
D. Social media can be used to gather intelligence for attacks.
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which of the following is the BEST method to obtain senior management buy-in for an information security investment?
A. Providing benchmark results from alternate vendors
B. Demonstrating the reduction in risk
C. Communicating the end-of-life support plan from vendor
D. Including sign-off from key stakeholders
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Which of the following is MOST important to include in contracts with key third-party providers?
A. Provisions to protect sensitive data
B. Right-to-terminate clauses
C. Financial penalties for breaches
D. Right-to-audit clauses
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
The FIRST step in a risk assessment for a business application is to:

A. identify the vulnerabilities of the application
B. identify the threats to the application
C. identify the assets used by the application.
D. rank the threats to the application
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Which of the following is the FIRST step in developing a business continuity plan (BCPY}?
A. Determine the business recovery strategy.
B. Identify critical business processes.
C. Determine available resources.
D. Identify the applications with the shortest recovery time objectives (RTOs).
Answer: (SHOW ANSWER)

NEW QUESTION: 159
For computer forensics evidence to be admissible in a court of law, the evidence MUST:
A. be stored in the original media.
B. meet standards of relevance
C. have integrity and accountability
D. be identifiable and reproducible
Answer: (SHOW ANSWER)

NEW QUESTION: 160
Which of the following is the MOST important driver when developing an effective information security strategy?

A. Benchmarking reports
B. Information security standards
C. Compliance requirements
D. Security audit reports
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Which of the following factors are the MAIN reasons why large networks are vulnerable?
A. Hacking and malicious software
B. Connectivity and complexity
C. Inadequate training and user errors
D. Network operating systems and protocols
Answer: (SHOW ANSWER)

NEW QUESTION: 162

An organization has selected an internationally recognized information security framework. Which of the following should be the PRIMARY basis for prioritizing the creation of related policies?
A. Steering committee recommendations
B. Correlation to business strategy
C. Budgetary requirements to support implementation
D. Regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 163
What should an information security manager do FIRST when made aware of a new regulation which may require the redesign of existing information security processes?
A. Develop a business case.
B. Develop a future state roadmap.
C. Perform a cost-benefit analysis.
D. Perform a gap analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
During which process is regression testing MOST commonly used?
A. Stress testing
B. Program development
C. Unit testing
D. System modification
Answer: (SHOW ANSWER)

NEW QUESTION: 165
What is the PRIMARY objective of triage within the incident response process?
A. Determination of incident impact
B. Timely reporting of incidents
C. Containment of incidents
D. Optimization of resources
Answer: (SHOW ANSWER)

NEW QUESTION: 166
An incident was detected where customer records were altered without authorization. The GREATEST concern for forensic analysis would be that the log data:
A. may not be time-synchronized.
B. has been disclosed.
C. may be modified.
D. could be temporarily available.
Answer: (SHOW ANSWER)

NEW QUESTION: 167
The MAIN reason for an information security manager to monitor industry level changes in the business and IT is to:
A. identify changes in the risk environment
B. change business objectives based on potential impact
C. update information security policies in accordance with the changes
D. evaluate the effect of the changes on the levels of residual risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which of the following presents the MOST significant challenge when classifying IT assets?
A. Vulnerabilities in information assets
B. Complex asset classification scheme
C. Information assets without owners
D. Disagreement between asset owners and custodians
Answer: (SHOW ANSWER)

NEW QUESTION: 169
When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:
A. report compliance to management
B. review the residual risk level
C. monitor for business changes.
D. implement controls to mitigate the risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Which of the following should be done FIRST when considering a new security initiative?
A. Conduct a feasibility study.
B. Perform a cost-benefit analysis.
C. Conduct a benchmarking exercise.

D. Develop a business case.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
An information security manager has discovered that a business unit is planning on implementing a new application and has not engaged anyone from the information security department. Which of the following is the BEST course of action?
A. Review and update the change management process.
B. Block the application from going into production.
C. Recommend involvement with the change manager.
D. Discuss the issue with senior leadership.
Answer: (SHOW ANSWER)

NEW QUESTION: 172
In a large organization, defining recovery time objectives (RTOs) is PRIMARILY the responsibility of;
A. the IT manager
B. the business unit manager.
C. senior management
D. the information security manager.
Answer: (SHOW ANSWER)

NEW QUESTION: 173
Which of the following BEST facilitates the monitoring of risk across an organization?
A. Threat assessments
B. Key risk indicators (KRIs)
C. Penetration testing
D. Risk appetite trends
Answer: (SHOW ANSWER)

NEW QUESTION: 174
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. Maturity models
C. Risk tolerance levels
D. Key risk indicators (KRIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which of the following BEST enables successful identification of a potential IT security incident?

A. Configuration management standards
B. Network intrusion detection systems (NIDS)
C. Event correlation
D. File integrity monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 176
For event logs to be acceptable for incident investigation, which of the following is MOST important to implement on all systems to establish a proper trail of evidence?
A. Source confidentiality
B. Time synchronization
C. Access to the logs
D. Event data integrity
Answer: (SHOW ANSWER)

NEW QUESTION: 177
When scoping a risk assessment, assets need lo be classified by
A. threats and opportunities
B. likelihood and impact.
C. redundancy and recoverability
D. sensitivity and criticality.
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which of the following is MOST effective in the strategic alignment of security initiatives?
A. Business leaders participate in information security decision making
B. Key information security policy are updated on a regular basis
C. A security steering committee is set up within the IT deployment.
D. Policies are created with input from business unit managers.
Answer: (SHOW ANSWER)

NEW QUESTION: 179
An awareness program is implemented to mitigate the risk of infections introduced through the use of social media Which of the following will BEST determine the effectiveness of the awareness program"
A. A quiz based on the awareness program materials
B. Employee attendance rate at the awareness program
C. A post-awareness program survey
D. A simulated social engineering attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 180

Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A. Establishing communication paths with vendors

B. Requiring security awareness training for vendor staff

C. Performing integration testing with vendor systems

D. Including service level agreements (SLAs) in vendor contracts

Answer: (SHOW ANSWER)

NEW QUESTION: 181

The BEST way to identify the risk associated with a social engineering attack is to

A. review single sign-on authentication logs

B. perform a business risk assessment of the email filtering system

C. test user knowledge of information security practices.

D. monitor the intrusion detection system (IDS)

Answer: (SHOW ANSWER)

NEW QUESTION: 182

Which of the following BEST protects against phishing attacks?

A. Network encryption

B. Security strategy training

C. Application whitelisting

D. Email filtering

Answer: (SHOW ANSWER)

NEW QUESTION: 183

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. Number of incident detected.

C. Number of emergencies declared

D. Elapsed time to resolve incidents

Answer: (SHOW ANSWER)

NEW QUESTION: 184
What should an information security manager do FIRST upon learning of a significant regulatory change that impacts how the organization should safeguard critical data?
A. Implement needed control changes.
B. Perform a gap analysis.
C. Report the regulatory change to senior management
D. Assess impact to industry peers.
Answer: (SHOW ANSWER)

NEW QUESTION: 185
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. Understanding the risk tolerance of corporate management
D. Integrating risk management into the software development life cycle
Answer: (SHOW ANSWER)

NEW QUESTION: 186
The effectiveness of an information security governance framework will BEST be enhanced if:
A. a culture of legal and regulatory compliance is promoted by management.
B. risk management is built into operational and strategic activities.
C. IS auditors are empowered to evaluate governance activities,
D. consultants review the information security governance framework
Answer: (SHOW ANSWER)

NEW QUESTION: 187
The PRIMARY responsibility to communicate with legal authorities regarding unauthorized disclosure of customer information should be defined in the:
A. information security policy.
B. disaster recovery plan (DRP).
C. Incident response plan
D. risk mitigation plan
Answer: (SHOW ANSWER)

NEW QUESTION: 188
Which aspect of an incident response plan will MOST effectively help to limit reputational damage when multiple media services are seeking a response following a major security breach?
A. The plan establishes clear lines of responsibility.

B. The plan has been reviewed by the media relations team.
C. The plan has been approved by executive management.
D. The plan complies with regulatory requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 189
An organization has decided to conduct a postmortem analysis after experiencing a loss from an information security attack. The PRIMARY purpose of this analysis should be to:
A. evaluate the impact.
B. document lessons learned.
C. update information security policies,
D. prepare for criminal prosecution.
Answer: (SHOW ANSWER)

NEW QUESTION: 190
An information security manager discovers that newly hired privileged users are not taking necessary steps to protect critical information at their workstations. Which of the following is the BEST way to address this situation?

A. Turn on logging and record user activity.
B. Communicate the responsibility and provide appropriate training.
C. Implement a data loss prevention (DLP) solution.
D. Publish an acceptable use policy and require signed acknowledgment.
Answer: (SHOW ANSWER)

NEW QUESTION: 191
Which of the following would BEST enable an information security manager to identify the risk associated with cloud-based solutions?
A. Assessing the solutions against the organization's security policies
B. Benchmarking with peer organizations using cloud solutions
C. Reviewing third-party audits of cloud service providers
D. Reviewing vendor adherence to service level agreements (SLAs)
Answer: (SHOW ANSWER)

NEW QUESTION: 192
Which of the following BEST enables effective information security governance9
A. Security-aware corporate culture
B. Established information security metrics
C. Periodic vulnerability assessments
D. Advanced security technologies
Answer: (SHOW ANSWER)

NEW QUESTION: 193
What is the BEST way for a customer to authenticate an e-commerce vendor?
A. Use a secure communications protocol for the connection.
B. Request email verification of the order
C. Encrypt the order using the vendor s private key
D. Verify the vendor's certificate with a certificate authority.
Answer: (SHOW ANSWER)

NEW QUESTION: 194
Which of the following should an information security manager do FIRST upon learning that a data loss prevention (DLP) scanner has identified payment card information (PCI) stored in cleartext within accounting file shares?
A. Initiate the incident response process.
B. Report the issue to senior management.
C. Perform an organization-wide risk assessment.
D. Assess the level of noncompliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 195
Which of the following factors is MOST likely to increase the chances of a successful social engineering attack?
A. Potential financial gain
B. Weak authentication for remote access
C. Knowledge of internal procedures
D. Technical skills
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Which of the following is the PRIMARY reason to conduct a post-incident review?
A. To notify regulatory authorities
B. To determine whether digital evidence is admissible
C. To aid in future risk assessments
D. To improve the response process
Answer: (SHOW ANSWER)

NEW QUESTION: 197
An organization is considering a self-service solution for the deployment of virtualized development servers.
Which of the following should be information security manager's PRIMARY concern?
A. Ability to maintain server security baseline
B. Segregation of servers from the production environment
C. Ability to remain current with patches
D. Generation of excessive security event logs
Answer: (SHOW ANSWER)

NEW QUESTION: 198
The BEST way to 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: (SHOW ANSWER)

NEW QUESTION: 199
Which of the following is the PRIMARY reason for conducting post-incident reviews?
A. To establish the cost of remediation
B. To determine the level of required remediation
C. To ensure regulatory compliance
D. To review lessons learned
Answer: (SHOW ANSWER)

NEW QUESTION: 200
Information security can BEST be enforced by making security:
A. a part of each employee's Job objectives.
B. a business process owner activity.
C. a flexible system of procedures and guidelines.
D. an integral component of corporate policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 201
Information security awareness programs are MOST effective when they are:
A. customized for each target audience
B. reinforced by computer-based training

C. conducted at employee orientation.
D. sponsored by senior management
Answer: (SHOW ANSWER)

NEW QUESTION: 202
Which of the following will provide the MOST accurate test results for a disaster recovery plan (DRP)?
A. Parallel test
B. Simulation test
C. Structured walk-through
D. Full interruption test
Answer: (SHOW ANSWER)

NEW QUESTION: 203
An intrusion prevention system (IPS) has reported a significant increase in the number of hacking attempts over the past month, though no systems have actually been compromised. Which of the following should the information security manager do FIRST?
A. Report the increase in hacking attempts to senior management.
B. Assess the risk associated with the hacking attempts.
C. Add more resources to monitor IPS alerts.
D. Validate the events identified by the IPS.
Answer: (SHOW ANSWER)

NEW QUESTION: 204
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 malware infections.
B. Track the trending of reported security incidents
C. Test end user response to simulated scenarios
D. Administer quizzes upon completion of training.
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Which of the following is a PRIMARY goal of an information security program?
A. To provide assurance that information security controls protect assets in accordance with the risk
B. To provide guidance to users, managers, and IT on organizational goals and objectives to protect data
C. To provide the highest level of protection available to an organization's information assets
D. To provide metrics to support management's assertion that information security is an organizational objective

Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which of the following architectures for e-business BEST ensures high availability?
A. A single point of entry allowing transactions to be received and processed quickly
B. Availability of an adjacent hot site and a standby server with mirrored copies of critical data
C. Automatic failover to the web site of another e-business that meets the user's needs
D. Intelligent middleware to direct transactions from a downed system to an alternative
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following BEST enables senior management to monitor the organization's risk exposure?
A. Monthly reporting on the IT risk register
B. Monthly reporting on new threats and vulnerabilities
C. Monthly reporting on information security incidents
D. Monthly reporting on changes to the risk profile
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Which of the following is an important criterion for developing effective key risk indicators (KRIs) to monitor information security risk?
A. The indicator should focus on IT and accurately represent risk variances.
B. The indicator should provide a retrospective view of risk impacts and be measured annually.
C. The indicator should possess a high correlation with a specific risk and be measured on a regular basis
D. The indicator should align with key performance indicators (KPIs) and measure root causes of process performance issues.
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Which of the following is MOST useful when prioritizing information security initiatives?
A. Input from senior management
B. Risk assessment results
C. Cost of noncompliance
D. Penetration testing results
Answer: (SHOW ANSWER)

NEW QUESTION: 210

A CEO requires that information security risk management is practiced at the organizational level through a central risk register. Which of the following is the MOST important reason to report a summary of this risk register to the board?

A. To ensure alignment with industry standards and trends
B. To facilitate alignment between risk management and organizational objectives
C. To ensure adequate funding is available for risk management and mitigation
D. To comply with the organization's regulatory and legal requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 211
Which of the following is the BEST methodology to manage access rights?
A. Two-factor authentication
B. Mandatory access control
C. Discretionary access control
D. Zero trust model
Answer: (SHOW ANSWER)

NEW QUESTION: 212
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. Regular testing of incident response plan
B. Accessing information security event data
C. Obtaining physical hardware for forensic analysis
D. Defining incidents and notification criteria
Answer: (SHOW ANSWER)

NEW QUESTION: 213
An organization is adopting a standardized corporate chat messaging technology to help facilitate communication among business units. Which of the following is an ESSENTIAL task associated with this initiative?
A. Reviewing existing organizational policies regarding the new technology

B. Restricting the use of the technology in departments with sensitive information
C. Enforcing encryption of chat communications
D. Increasing security and operational staffing to support the technology
Answer: (SHOW ANSWER)

NEW QUESTION: 214
Which of the following roles should be separated?
A. Data security and database administration
B. Firewall management and security operations
C. Systems analysis and application programming
D. Help desk and security administration
Answer: (SHOW ANSWER)

NEW QUESTION: 215
Which of the following should be the PRIMARY outcome of an information security program'?
A. Threat reduction
B. Strategic alignment
C. Cost reduction
D. Risk elimination
Answer: (SHOW ANSWER)

NEW QUESTION: 216
Which of the following would be MOST helpful in gaming support for a business case for an Information security initiative9
A. Presenting a solution comparison matrix
B. Demonstrating organizational alignment
C. Referencing control deficiencies
D. Emphasizing threats to the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 217
An email digital signature will:
A. prevent unauthorized modification of an email message.
B. verify to recipients the integrity of an email message.
C. protect the confidentiality of an email message.
D. automatically correct unauthorized modification of an email message.
Answer: (SHOW ANSWER)