ISACA.CISM.v2021-07-06.q400

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	400
Version:	v2021-07-06
# of views:	2891
# of Questions views:	117475
https://www.freecram.net/torrent/ISACA.CISM.v2021-07-06.q400.html	

NEW QUESTION: 1
An organization wants to implement an emerging technology to support operations. What should the information security manager do FIRST when ..... recommendation?
A. Develop a business case.
B. Assess the potential security impact.
C. Review key risk indicators (KRIs).
D. Review existing security policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Business units within an organization are resistant to proposed changes to the information security program.
Which of the following is the BEST way to address this issue?
A. Implementing additional security awareness training
B. Including business unit representation on the security steering committee
C. Publishing updated information security policies
D. Communicating critical risk assessment results to business unit managers
Answer: (SHOW ANSWER)

NEW QUESTION: 3
The MOST important reason to maintain key risk indicators (KRIs) is that:
A. they help assess the performance of the security program.
B. threats and vulnerabilities continuously evolve.
C. management uses them to make informed business decisions.
D. they are needed to verify compliance with laws and regulations
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which of the following is the NEXT course of action for an incident response team if an Incident cannot be investigated in the allocated time?
A. Activate the business continuity plan (BCP).
B. Discontinue the investigation.
C. Request an exception to the service level agreement (SLA).
D. Escalate to senior management for resolution.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Following a recent acquisition, an information security manager has been requested to address the outstanding risk reported early in the acquisition process. Which of the following is the manager s BEST course of action?
A. Perform a vulnerability assessment of the acquired company s infrastructure.
B. Re-assess the outstanding risk of the acquired company.
C. Re-evaluate the risk treatment plan for the outstanding risk.
D. Add the outstanding risk to the acquiring organization's risk registry
Answer: (SHOW ANSWER)

NEW QUESTION: 6
The MAIN consideration when designing an incident escalation plan should be ensuring that:
A. requirements cover forensic analysis.
B. information assets are classified.
C. high-impact risks have been identified.
D. appropriate stakeholders are involved,
Answer: (SHOW ANSWER)

NEW QUESTION: 7
An organization has detected potential risk emerging from noncompliance with new regulations in its industry.
Which of the following is the MOST important reason to report this situation to senior management?
A. An external review of the risk nods to be conducted
B. Specific monitoring controls need to be implemented
C. The risk profile needs to be updated
D. A benchmark analysis needs to be performed.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
When creating an information security governance program, which of the following will BEST enable the organization to address regulatory compliance requirements?

A. A security control framework
B. An approved security strategy plan
C. Input from the security steering committee
D. Guidelines for processes and procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following is the MOST effective way to facilitate the implementation of IT security program objectives?
A. Designing a compulsory IT security training program for all employees
B. Establishing a steering committee with executive and business involvement
C. Developing a suite of policy, standards, and procedure documents
D. Creating a help desk and change management platform
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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 ensure that messages to external parties are complete and accurate
C. To automate communication with external parties without delay
D. To communicate efficiently and consistently
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which of the following would provide senior management with the BEST overview of the performance of information security risk treatment options?
A. Before-and-after heat maps
B. Detailed risk analysis of the treatments
C. individual risk assessments
D. Analysis of recent incident
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following is the MOST useful metric for determining how well firewall logs are being monitored?
A. The number of port scanning attempts
B. The number of log entries reviewed
C. The number of dropped malformed packets
D. The number of investigated alerts
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following is the BEST way to monitor for advanced persistent threats (APT) in an organization?
A. Network with peers in the industry to share information
B. Search for anomalies in the environment.
C. Search for threat signatures in the environment.
D. Browse the Internet to learn of potential events.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Establishing which of the following is the BEST way of ensuring that the emergence of new risk is promptly identified?
A. Incident monitoring activities
B. Risk monitoring processes
C. Regular risk repotting
D. Change control procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 15
The PRIMARY advantage of a network intrusion detection system (IDS) is that it can:
A. detect network vulnerabilities
B. block undesirable network traffic
C. identify an attack on the network.
D. simulate denial-of-service attacks.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following should be the PRIMARY goal of an Information security manager when designing Information security policies?
A. Achieving organizational objectives
B. Reducing organizational security risk
C. Minimizing the cost of security controls
D. Improving the protection of information
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following is a PRIMARY goal of an information security program?
A. To provide metrics to support management's assertion that information security is an organizational objective
B. To provide the highest level of protection available to an organization's information assets
C. To provide assurance that information security controls protect assets in accordance with the risk
D. To provide guidance to users, managers, and IT on organizational goals and objectives to protect data
Answer: (SHOW ANSWER)

NEW QUESTION: 18
The MOST important reason that security risk assessments should be conducted frequently throughout an organization is because:
A. controls should be regularly tested.
B. compliance with legal and regulatory standards should be reassessed.
C. control effectiveness may weaken.
D. threats to the organization may change.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following is the- BEST method to determine whether an information security program meets an organization s business objectives?
A. Review against international security standards.
B. Implement performance measures.
C. Perform a business impact analysis (BIA)
D. Conduct an annual enterprise-wide security evaluation.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
An organization plans to acquire and implement a new web-based solution to enhance service functionality.
Which of the following is the BEST way to ensure that information handled by the solution is secure?

A. Embed security requirements throughout the life cycle of the solution.
B. Conduct a security audit before implementing the solution in production.
C. Integrate the organization's security requirements into the contract.
D. Adopt secure coding practices during the solution's development.

Answer: (SHOW ANSWER)

NEW QUESTION: 21
The MOST effective way to determine the resources required by internal Incident response teams is to
A. test response capabilities with event scenarios.
B. benchmark against other incident management programs
C. request guidance (rom incident management consultants.
D. determine the scope and charter of incident response
Answer: (SHOW ANSWER)

NEW QUESTION: 22
A new organization has been hit with a ransomware attack that is critically impacting its business operations.
The organization does not yet have a proper incident response plan, but it does have a backup procedure for restoration of data. Which of the following should be the FIRST course of action?
A. Recommend that management pay the ransom.
B. Establish an incident response plan.
C. Contact the legal department.
D. Isolate the affected system.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which of the following is the PRIMARY purpose for defining key performance indicators (KPIs) for a security program?
A. To ensure controls meet regulatory requirements
B. To evaluate the performance of security staff
C. To compare security program effectiveness to best practice
D. To measure the effectiveness of the security program
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
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. ensure the organization's ownership of data and management of the device.
D. develop remote wipe capabilities and procedures.
Answer: (SHOW ANSWER)

NEW QUESTION: 25

An organization is planning to create a website that will collect site-visitor details from around the world and use them as marketing lists for operations in several countries. Which of the following should be of MOST concern to the information security manager?
A. Legislation regarding marketing in foreign countries
B. Privacy laws in each of the countries using the details for marketing
C. Wording of the website's policy statement on how the details will be used
D. Using cryptography for transborder data flow
Answer: (SHOW ANSWER)

NEW QUESTION: 26
When an organization lacks internal expertise to conduct highly technical forensics investigations, what is the BEST way to ensure effective and timely investigations following an information security incident?
A. Provide forensics training to the information security team.
B. Retain a forensics firm prior to experiencing an incident.
C. Purchase forensic standard operating procedures.
D. Ensure the incident response policy allows hiring a forensics firm.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Before final acceptance of residual risk, what is the BEST way for an information security manager to address risk factors determined to be lower than acceptable risk levels?
A. Ask senior management to increase the acceptable risk levels
B. Evaluate whether an excessive level of control is being applied.
C. Ask senior management to lower the acceptable risk levels.
D. Implement more stringent countermeasures.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following would BEST mitigate identified vulnerabilities in a timely manner?
A. Action plan with responsibilities and deadlines
B. Monitoring of key risk indicators (KRIs)
C. Continuous vulnerability monitoring tool
D. Categorization of the vulnerabilities based on system's criticality
Answer: (SHOW ANSWER)

NEW QUESTION: 29
In which of the following situations is it MOST important to escalate an incident response to senior management?
A. The impact of the incident exceeds the organization's risk tolerance.
B. The owner of the affected business function is not available.

C. The incident impacts a business-critical system.
D. The time-related service levels for response are below risk threshold levels.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
After assessing risk, the decision to treat the risk should be based PRIMARILY on:
A. whether the level of risk exceeds inherent risk.
B. availability of financial resources.
C. the criticality of the risk.
D. whether the level of risk exceeds risk appetite.
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of integrity?
A. Ensuring encryption for data in transit
B. Implementing a data classification schema
C. Enforcing service level agreements (SLAs)
D. Utilizing a formal change management process
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following would provide the BEST input to a business case for a technical solution to address potential system vulnerabilities?
A. Vulnerability scan results
B. Risk assessment
C. Business impact analysis (BIA)
D. Penetration test results
Answer: (SHOW ANSWER)

NEW QUESTION: 33

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

A. More employees and stakeholders are attending security awareness programs.

B. The number of threats has been reduced.

C. Management's attention and budget are now focused on risk reduction.

D. The number of vulnerability false positives is decreasing.

Answer: (SHOW ANSWER)

NEW QUESTION: 34

With limited resources in the information security department which of the following is the BEST approach for managing security risk?

A. Implement technical solutions to automate security management activities.

B. Hire additional information security staff.

C. Engage a third-party company to provide security support.

D. Prioritize security activities and report to management

Answer: (SHOW ANSWER)

NEW QUESTION: 35

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. Employee attendance rate at the awareness program

B. A post-awareness program survey

C. A simulated social engineering attack

D. A quiz based on the awareness program materials

Answer: (SHOW ANSWER)

NEW QUESTION: 36

A large organization is considering a policy that would allow employees to briog their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

A. higher costs in supporting end users.

B. decrease in end user productivity.

C. impact on network capacity.

D. lack of a device management solution.

Answer: (SHOW ANSWER)

NEW QUESTION: 37

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

A. remain unchanged to avoid variations across the organization

B. be updated to address emerging threats and vulnerabilities.
C. not deviate from industry best practice baselines.
D. be changed for different subsets of the systems to minimize impact,
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which is MOST important when contracting an external party to perform a penetration test?
A. Increase the frequency of log reviews.
B. Provide network documentation.
C. Obtain approval from IT management.
D. Define the project scope
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following BEST indicates the value a purchased information security solution brings to an organization?
A. Degree to which the solution matures the information security program
B. Alignment to security threats and risks
C. Costs and benefits of the solution calculated over time
D. Cost savings the solution brings to the information security department
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following is the PRIMARY goal of a risk management program?
A. Manage the business impact of inherent risks.
B. Reduce the organization s risk appetite
C. Implement preventive controls against threats
D. Manage compliance with organizational polices.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value c*n be mitigated by:
A. using a secret key m conjunction with the hash algorithm.
B. requiring the recipient to use a different hash algorithm,
C. using the senders public key to encrypt the message.
D. generating hash output that is the same size as the original message,
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42

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. Integrate organization's security requirements into project management.
B. Participate in project initiation, approval, and funding.
C. Conduct security reviews during design, testing and implementation
D. Develop good communications with the project management office
Answer: (SHOW ANSWER)

NEW QUESTION: 43
The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the GREATEST when:
A. operations and monitoring are handled by different teams.
B. IDS sensors are misconfigured.
C. The IT infrastructure is diverse.
D. standard operating procedures are not formalized.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Which of the following is the MOST important security consideration when using Infrastructure as a Service (IaaS)?
A. Compliance with internal standards
B. Backup and recovery strategy
C. Segmentation among tenants
D. User access management
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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. Identify potential incident impact.
B. Implement additional incident response monitoring tools.
C. Initiate the incident response process.
D. Assess the level of the residual risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
The PRIMARY purpose of aligning information security with corporate governance objectives is to:
A. identity an organization s tolerance for risk
B. build capabilities to improve security processes

C. re-align roles and responsibilities.
D. consistently manage significant areas of risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 47
The MOST effective way to communicate the level of impact of information security risks on organizational objectives is to present:
A. a risk heat map.
B. detailed threat analysis results.
C. risk treatment options.
D. business impact analysis (BIA) results.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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. Conduct a vulnerability assessment on the devices.
C. Assess risks introduced by the technology
D. Research mobile device management (MDM) solutions.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
An organization's information security strategy for the coming year emphasizes reducing the risk of ransomware. Which of the following would be MOST helpful to support this strategy?
A. Perform a controls gap analysis.
B. Strengthen security controls for the IT environment.
C. Provide relevant training to all staff.
D. Create a penetration testing plan
Answer: (SHOW ANSWER)

NEW QUESTION: 50

Which of the following should be done FIRST when implementing policies to address an upcoming new data privacy regulation?

A. Segregate systems processing personal data from other systems on the network-
B. Prohibit further collection of personal data until the regulation is implemented.
C. Understand which types of personal data are covered by the new regulation.
D. Understand what technologies are required for personal data protection.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Which of the following is MOST important to present to stakeholders to help obtain support for implementing a new information
A. An overview of competitors' information security strategies
B. The potential impact of current threats
C. An assessment of current technological exposures
D. A statement of generally accepted good practices
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following is the MOST effective method of preventing deliberate internal security breaches?
A. Screening prospective employees
B. Well-designed intrusion detection system (IDS)
C. Biometric security access control
D. Well-designed firewall system
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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. Antivirus program and incident response plans
B. Remediation schedule for patch management
C. Measures taken to prevent the risk of a data breach
D. Disaster recovery and continuity program plans
Answer: (SHOW ANSWER)

NEW QUESTION: 54
When an organization and its IT-hosting service provider are establishing a contract with each other, it is MOST important that the contract includes:
A. penalties for noncompliance with security policy
B. each party s security responsibilities.

C. recovery time objectives (RTOs).
D. details of expected security metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following is the BEST way to address any gaps identified during an outsourced provider selection and contract negotiation process?
A. Perform continuous gap assessments.
B. Implement compensating controls.
C. Include audit rights in the service level agreement (SLA).
D. Make the provider accountable for security and compliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
For computer forensics evidence to be admissible in a court of law, the evidence MUST:
A. meet standards of relevance
B. be stored in the original media.
C. be identifiable and reproducible
D. have integrity and accountability
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which of the following is a PRIMARY responsibility of a data owner?
A. Approving access to information
B. Conducting data privacy impact assessments
C. Performing user access audits
D. Processing entitlement changes
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which of the following provides the GREATEST assurance that an organization allocates appropriate resources to respond to information security events?
A. Incident classification procedures
B. An approved IT staffing plan
C. Threat analysis and intelligence reports
D. Information security policies and standards
Answer: (SHOW ANSWER)

NEW QUESTION: 59
When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure that the:

A. forensic investigation software is loaded on the server.
B. server is backed up to the network.
C. server is unplugged from power.
D. integrity of evidence is preserved.
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Which of the following is MOST important to consider when handling digital evidence during the forensics investigation of a cybercrime?

A. Local regulations
B. Business strategies
C. Industry best practices
D. Global standards
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which of the following should be the FIRST step of incident response procedures?
A. Classify the event depending on seventy and type.
B. Perform a risk assessment to determine the business impact.
C. Identify if there is a need for additional technical assistance.
D. Evaluate the cause of the control failure.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
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. improved efficiencies of security operations.
D. more effective security risk management processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following should be the PRIMARY consideration when selecting a recovery site?
A. Recovery time objective
B. Regulatory requirements
C. Geographical location
D. Recovery point objective
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
An information security manager is evaluating the key risk indicators (KRIs) for an organization s information security program. Which of the following would be the information security manager s GREATEST concern?
A. Multiple KRIs for a single control process
B. Lack of formal KRI approval from IT management
C. Undefined thresholds to trigger alerts
D. Use of qualitative measures
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following BEST indicates that information security will be considered when new IT technologies are implemented across an organization?
A. Employees receive information security awareness training.
B. IT employee job descriptions include information security roles and responsibilities.
C. The information security function reports to the chief information officer.
D. The information security manager is on the IT architecture review board.
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following will BEST enable an effective information asset classification process?
A. Reviewing the recovery time objective (RTO) requirements of the asset
B. Including security requirements in the classification process
C. Analyzing audit findings
D. Assigning ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following is the MOST important outcome of a well-implemented awareness program?
A. The number of successful social engineering attacks is reduced.
B. The board is held accountable for risk management.
C. The number of reported security incidents steadily decreases.

D. Help desk response time to resolve incidents is improved.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
An information security manager has been asked to identify potential threats to the organization's information.
Which of the following should be done FIRST'
A. Review cyber insurance coverage.
B. Engage a third-parry consultant
C. Select a governance framework.
D. Develop a risk profile.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Which of the following is MOST relevant for an information security manager to communicate to business units?
A. Threat assessments
B. Risk ownership
C. Vulnerability assessments
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Who within an organization is accountable for ensuring incident notification and escalation processes are in place?

A. Data owner
B. Senior management
C. Information security manager
D. Security operations center management
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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. Document the incident response plan
C. Define communication processes
D. Conduct incident response plan testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
The MOST important factors in determining the scope and timing for testing a business continuity plan are:
A. the experience level of personnel and the function location.
B. prior testing results and the degree of detail of the business continuity plan
C. manual processing capabilities and the test location
D. the importance of the function to be tested and the cost of testing,
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following has the MOST influence on an organization's adoption of information security policies?
A. Established key performance indicators (KPIs)
B. A comprehensive security awareness program
C. Demonstrated senior management commitment
D. Enforcement of penalties for noncompliance
Answer: (SHOW ANSWER)

NEW QUESTION: 74
An organization recently implemented a data loss prevention (DLP) system. A senior business executive has complained that the system seriously impedes departmental effectiveness. What is the information security manager's BEST course of action?
A. Request risk acceptance.
B. Perform a risk assessment.
C. Review alternative controls.
D. Change the DLP system.
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following is the BEST way to reduce the risk of a ransomware attack?
A. Confirm backups are not connected to the network.
B. Authenticate inbound email and enable strong content filtering
C. Perform a network vulnerability assessment.
D. Perform regular backups and validate the restoration process
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following is the MOST important reason for performing vulnerability assessments periodically?
A. Management requires regular reports.
B. The environment changes constantly.

C. Technology risks must be mitigated.
D. The current threat levels are being assessed.
Answer: (SHOW ANSWER)

NEW QUESTION: 77
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. business owners.
C. senior management.
D. the security operations center.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following is the MOST effective way for senior management to support the integration of information security governance into corporate governance?
A. Develop the information security strategy based on the enterprise strategy
B. Establish a storing committee with representation from across the organization.
C. Promote organization-wide information security awareness campaigns.
D. Appoint a business manager as head of information security
Answer: (SHOW ANSWER)

NEW QUESTION: 79
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. Develop key risk indicators (KRIs).
B. Create an information security action plan.
C. Determine information security requirements for the cloud.
D. Assess the risk associated with the cloud services.
Answer: (SHOW ANSWER)

NEW QUESTION: 80

During a post-incident review, the sequence and correlation of actions must be analyzed PRIMARILY based on:

A. a consolidated event timeline
B. interviews with personnel.
C. documents created during the incident.
D. logs from systems involved.
Answer: (SHOW ANSWER)

NEW QUESTION: 81
A risk management program will be MOST effective when:
A. business units are involved in risk assessments,
B. assessments are repeated periodically
C. risk appetite is sustained for a long period risk
D. risk assessments are conducted by a third party.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?
A. Evaluating the provider s security incident response plan
B. Continuous monitoring of An information security risk profile
C. Ensuring the provider's roles and responsibilities are established
D. Requiring periodic self-assessments by the provider
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following BEST enables new third-party suppliers to support an organization's information security objectives?
A. Requiring approval of new suppliers by the information security manager
B. Conducting security awareness training courses for third parties
C. Mandating a right-to-audit clause in supplier contracts
D. Addressing security risk in the supplier sourcing process
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following presents the GREATEST concern to the information security manager when using account locking features on an online application? It can increase vulnerability to.
A. brute force attacks.
B. denial of service.
C. phishing.
D. social engineering.

Answer: (SHOW ANSWER)

NEW QUESTION: 85
It is MOST important tot an information security manager to ensure that security risk assessments are performed:
A. during a root cause analysis
B. as part of the security business case
C. In response to the threat landscape,
D. consistently throughout the enterprise.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
In an organization that has undergone an expansion through an acquisition, which of the following would BEST secure the enterprise network?
A. Business or rote-based segmentation
B. Using security groups
C. Log analysis of system access
D. Encryption of data traversing networks
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Mitigating technology risks to acceptable levels should be based PRIMARILY upon:
A. business process requirements.
B. information security budget.
C. legal and regulatory requirements.
D. business process reengineering.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following is MOST important to consider when developing a security awareness program in an organization?
A. Established key risk indicators (KRIs)
B. Targeted monthly deliverables
C. Target audience demographics
D. Industry benchmarks
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Which of the following would BEST enable management to be aware of an electronic breach to an externally hosted database?
A. Review independent audit reports of the vendors data center environment.

B. Implement a dedicated firewall configured to block suspicious activity.
C. Obligate the vendor to report suspicious activity and database breaches.
D. Implement tog monitoring of the database environment for suspicious activity.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
In a large organization requesting outsourced services, which of the following contract clauses is MOST important to the information security manager?

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

NEW QUESTION: 91
Which of the following is the MOST important function of information security?
A. Reducing the financial impact of security breaches
B. Preventing security incidents
C. Managing risk to the organization
D. Identifying system vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 92
After undertaking a security assessment of a production system, the information security manager is MOST likely to:
A. establish an overall security program that minimizes the residual risks of that production system
B. inform the development team of any residual risks and together formulate risk reduction measures.
C. inform the system owner of any residual risks and propose measures to reduce them.
D. inform the IT manager of the residual risks and propose measures to reduce them.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
What is the role of the information security manager in finalizing contract negotiations with service providers?
A. To ensure that clauses for periodic audits are included
B. To obtain a security standard certification from the provider
C. To perform a risk analysis on the outsourcing process
D. To update security standards for the outsourced process
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
What is the MOST important role of an organization's data custodian in support of the information security function?
A. Approving access rights to departmental data
B. Assessing data security risks to the organization
C. Evaluating data security technology vendors
D. Applying approved security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following is the MOST important consideration for designing an effective information security governance framework?
A. Security policy provisions
B. Continuous audit cycle
C. Defined security metrics
D. Security controls automation
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following should the information security manager do FIRST after a security incident has been reported?
A. Retrieve the information needed to confirm the incident.
B. Identify the scope and size of the affected environment.
C. Determine the degree of loss resulting from the incident.
D. Identify the possible source of attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Human resources is evaluating potential Software as a Service (SaaS) cloud services, Which of the following should the information security manager do FIRST to support..
A. Conduct a security audit on the cloud service providers.

B. Perform a cost-benefit analysis of using cloud services.
C. Perform a risk assessment of adopting cloud services.
D. Review the cloud service providers" controls reports.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
The frequency of conducting business impact analysis (BIA) should PRIMARILY be based on:
A. changes in regulatory requirements.
B. business continuity plan (BCP) testing.
C. changes in business processes.
D. the number of security incidents.
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?
A. Ratio of tested applications to total applications
B. Ratio of successful to unsuccessful tests
C. Ratio of recovery-plan documents to total applications
D. Number of published application-recovery plans
Answer: B (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following BEST determines an information asset's classification?
A. Directives from the data owner
B. Criticality to a business process
C. Cost of producing the information asset
D. Value of the information asset to competitors
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Several significant risks have been identified after a centralized risk register was compiled and prioritized. The information security manager's MOST important action is to:
A. ensure that employees are aware of the risk.
B. consult external third parties on how to treat the risk
C. design and implement controls to reduce the risk.
D. provide senior management with risk treatment options.
Answer: (SHOW ANSWER)

NEW QUESTION: 102
The selection of security controls is PRIMARILY linked to:

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

NEW QUESTION: 103
Which of the following is the BEST criterion to use when classifying assets?
A. The market value of the assets
B. Value of the assets relative to the organization
C. Annual loss expectancy (ALE)
D. Recovery time objective (RTO)
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which of the following is MOST helpful in integrating information security governance with corporate governance?
A. Assigning the implementation of information security governance to the steering committee
B. Aligning the information security governance to a globally accepted framework
C. Providing independent reports of information security efficiency and effectiveness to the board
D. Including information security processes within operational and management processes
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following will BEST help to ensure security is addressed when developing a custom application?
A. Integrating security requirements into the development process
B. Requiring a security assessment before implementation
C. Integrating a security audit throughout the development process
D. Conducting security training for the development staff
Answer: (SHOW ANSWER)

NEW QUESTION: 106
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: (SHOW ANSWER)

NEW QUESTION: 107
An information security manager is concerned that executive management does not su the following is the BEST way to address this situation?
A. Demonstrate alignment of the information security function with business needs.
B. Report the risk and status of the information security program to the board.
C. Escalate noncompliance concerns to the internal audit manager
D. Revise the information security strategy to meet executive management expectations.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which of the following is the BEST evidence that proper security monitoring controls are in place?
A. The intrusion detection system (IDS) generates potential alerts.
B. Incidents are contained before they cause damage
C. Staff regularly report suspicious activity.
D. Mature escalation procedures are in place for incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 109
After a risk has been mitigated, which of the following is the BEST way to help ensure residual risk remains within an organization's established risk tolerance?
A. Perform a business impact analysis (BIA).
B. Monitor the security environment for changes in risk.
C. Conduct programs to promote user risk awareness
D. Introduce new risk scenarios to test program effectiveness.
Answer: (SHOW ANSWER)

NEW QUESTION: 110
The BEST way to improve the effectiveness of responding to and communicating security incidents is to ensure:

A. senior management is notified at the onset of incident response.
B. additional staff are trained and available to assist with incident response.
C. the incident response plan is regularly tested.

D. the IT budget includes funding for SIEM tools to log incidents.
Answer: (SHOW ANSWER)

NEW QUESTION: 111
An information security manager is preparing an incident response plan. Which of the following is the MOST important consideration when responding to an incident involving sensitive customer data?
A. The ability to recover from the incident in a timely manner
B. The assignment of a forensics team
C. Following defined post-incident review procedures
D. The ability to obtain incident information in a timely manner
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Which of the following BEST describes an intrusion detection system (IDS) that learns the system behaviors prior to detecting potential intrusions?
A. Host-based IDS
B. Network-based IDS
C. Application-based IDS
D. Anomaly-based IDS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
Which of the following is MOST important to include in contracts with key third-party providers?
A. Right-to-terminate clauses
B. Right-to-audit clauses
C. Provisions to protect sensitive data
D. Financial penalties for breaches
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which of the following is the MOST effective way to communicate information security risk to senior management?
A. Business impact analysis (BIA)
B. Balanced scorecard
C. Key performance indicators (KPIs)
D. Heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 115

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

NEW QUESTION: 116
The PRIMARY purpose of vulnerability assessments is to:
A. test intrusion detection systems (IDS) and response procedures
B. determine the impact of potential threats,
C. detect deficiencies that could lead to a system compromise.
D. provide clear evidence that the system is sufficiently secure.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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. Require remote wipe capabilities for devices.
C. Conduct security awareness training.
D. Enforce passwords and data encryption on the devices.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Who is MOST important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data toss?
A. An independent auditor for identification of control deficiencies
B. A forensics expert for evidence management
C. A damage assessment expert for calculating losses
D. A penetration tester to validate the attack
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Failure to include information security requirements within the build/buy decision would MOST likely result in the need for:
A. more stringent source programming standards.
B. compensating controls in the operational environment.
C. security scanning of operational platforms
D. commercial product compliance with corporate standards.

Answer: (SHOW ANSWER)

NEW QUESTION: 120
What should be the PRIMARY basis for prioritizing incident containment?
A. The recovery cost of affected assets
B. The business value of affected assets
C. Input from senior management
D. Legal and regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 121
The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:
A. maintain compliance with industry best practices.
B. maintain an accurate record of users access rights
C. assign accountability for transactions made with the user's ID.
D. serve as evidence of security awareness training.
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Which of the following is the BEST way to determine if an information security program aligns with corporate governance?
A. Survey end users about corporate governance.
B. Review the balanced scorecard.
C. Review information security policies.
D. Evaluate funding for security initiatives.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following is MOST important to the successful development of an information security strategy?
A. An implemented development life cycle process

B. Approved policies and standards
C. A well-implemented governance framework
D. Current state and desired objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which of the following would present the GREATEST need to revise information security poll'
A. Implementation of a new firewall
B. A merger with a competing company
C. An increase in reported incidents
D. Changes in standards and procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 125
A business unit has updated its long-term business plan to include a strategy of upgrading information management systems to increase productivity. To support this initiative, what should be the PRIMARY basis for updating the corresponding. information security strategy?
A. The IT strategy
B. IT risk assessment results
C. The information security framework
D. The business strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 126
The FIRST step in a risk assessment for a business application is to:
A. identify the threats to the application
B. identify the assets used by the application.
C. rank the threats to the application
D. identify the vulnerabilities of the application
Answer: (SHOW ANSWER)

NEW QUESTION: 127
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:
A. perform a gap analysis.
B. review information security policies
C. review the state of security awareness.
D. perform a risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 128

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

A. Heat map

B. Maturity level

C. Audit findings

D. Penetration test results

Answer: A (LEAVE A REPLY)

NEW QUESTION: 129

Which of the following is the BIST course of action for the information security manager when residual risk is above the acceptable level of risk?

A. Perform a cost-benefit analysis.

B. Recommend additional controls.

C. Defer to business management.

D. Carry out a risk assessment

Answer: B (LEAVE A REPLY)

NEW QUESTION: 130

A third-party contract signed by a business unit manager failed to specify information security requirements Which of the following is the BEST way for an information security manager to prevent this situation from reoccurring?

A. Provide information security training to the business units

B. Integrate information security into the procurement process

C. Inform business unit management of the information security requirements.

D. Involve the information security team in contract negotiations

Answer: (SHOW ANSWER)

NEW QUESTION: 131

An organization plans to leverage popular social network platforms to promote its products and services.

Which of the following is the BEST course of action for the information security manager to support this initiative?

A. Conduct vulnerability assessments on social network platforms

B. Assess the security risk associated with the use of social networks

C. Establish processes to publish content on social networks

D. Develop security controls for the use of social networks

Answer: (SHOW ANSWER)

NEW QUESTION: 132

Which of the following is MOST useful to include in a report to senior management on a regular basis to demonstrate the effectiveness of the information security program?

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

NEW QUESTION: 133
Which of the following BIST validates that security controls are implemented in a new business process?
A. Verify the use of a recognized control framework
B. Review the process for conformance with information security best practices
C. Assess the process according to information security policy
D. Benchmark the process against industry practices
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which of the following is MOST important when prioritizing an information security incident?
A. Organizational risk tolerance
B. Criticality of affected resources
C. Cost to contain and remediate the incident
D. Short-term impact to shareholder value
Answer: B (LEAVE A REPLY)

NEW QUESTION: 135
Which of the following is the MOST effective method to help ensure information security incidents are reported?
A. Integrating information security language in corporate compliance rules
B. Providing information security awareness training to employees
C. Implementing an incident management system
D. Integrating information security language in conditions of employment
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following should be the GREATEST concern when considering launching a counterattack in response to a network attack?
A. Legal ramifications
B. Digital evidence contamination
C. Incident impact escalation
D. Denial of service attacks on the external source
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which of the following would BEST protect against web-based cross-domain attacks?
A. Network addressing scheme
B. Encryption controls
C. Application controls
D. Database hardening
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which of the following defines the MOST comprehensive set of security requirements for a newly developed information system?
A. Audit findings
B. Baseline controls
C. Key risk indicators (KRIs)
D. Risk assessment results
Answer: (SHOW ANSWER)

NEW QUESTION: 139
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. Remove overlapping security controls
C. Prioritize security projects based on risk.
D. Create a business case appeal decision.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
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. Business case
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Which of the following is the FIRST task when determining an organization's information security profile?
A. Establish security standards.
B. Complete a threat assessment
C. List administrative privileges.
D. Build an asset inventory.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
Organization XYZ. a lucrative, Internet-only business, recently suffered a power outage that lasted 2 hours.
The organization s data center was unavailable in the interim. In order to mitigate risk in the MOST cost-efficient manner, the organization should:
A. plan to operate at a reduced capacity from the primary place of business.
B. set up a duplicate business center in a geographically separate area.
C. install an uninterruptible power supply (UPS) and generator.
D. create an FT hot site with immediate fail-over capability.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
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. Security awareness training
C. A network intrusion detection system (NIDS)
D. Placing the e-mail server on a screened subnet
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Senior management learns of several web application security incidents and wants to know the exposure risk to the organization. What is the information security manager's BEST course of action?
A. Perform a vulnerability assessment.
B. Review audit logs from IT systems.
C. Assess IT system configurations
D. Activate the incident response plan

Answer: A (LEAVE A REPLY)

NEW QUESTION: 145
Which of the following provides the BEST indication that the information security program is in alignment with enterprise requirements?
A. An IT governance committee is m place.
B. The information security manager reports to the chief executive officer.
C. The security strategy is benchmarked with similar organizations
D. Security strategy objectives are defined in business terms.
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Information security governance is PRIMARILY driven by which of the following?
A. Business strategy
B. Technology constraints
C. Litigation potential
D. Regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 147
After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?
A. Risk heat map
B. Gap analysis
C. Balanced scorecard
D. Recent audit results
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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. Cost-benefit analysis
B. Cost of software
C. Implementation timeframe
D. Industry benchmarks
Answer: (SHOW ANSWER)

NEW QUESTION: 149
When developing an information security governance framework, which of the following should be the FIRST activity?

A. Integrate security within the system's devetoojtam life cycle process.
B. Develop policies and procedures to support the framework.
C. Align the information security program with the organization's other risk and control activities.
D. Develop response measures to detect and ensure the closure of security breaches.
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Which of the following BEST promotes stakeholder accountability in the management of information security risks?

A. Targeted security procedures
B. Establishment of security baselines
C. Establishment of information ownership
D. Regular reviews for noncompliance
Answer: (SHOW ANSWER)

NEW QUESTION: 151
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. Remediate the vulnerability.
B. Perform a risk assessment.
C. Activate the incident response team.
D. Isolate potentially vulnerable systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 152
The PRIMARY goal of a security infrastructure design is the:
A. elimination of risk exposures.
B. reduction of security incidents.
C. protection of corporate assets
D. optimization of IT resources
Answer: (SHOW ANSWER)

NEW QUESTION: 153
Which of the following is the BEST way to provide management with meaningful information regarding the performance of the information security program against strategic objectives?
A. Publish the information security strategy across the organization.
B. Establish a balanced scorecard dashboard.
C. Develop an information security heat map.
D. Issue periodic reports to demonstrate compliance with security standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
The BEST way to establish a security baseline is by documenting:
A. the desired range of security settings
B. the organization's preferred security level.
C. a framework of operational standards
D. a standard of acceptable settings
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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. Include industry benchmarking comparisons.
C. Provide the estimated return on investment (ROI).
D. Include historical data of reported incidents.
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Which of the following should be the FIRST step to ensure system updates are applied in a timely manner?
A. Cross-reference all missing patches to establish the date each patch was introduced.
B. Establish a risk-based assessment process for prioritizing patch implementation.
C. Create a regression test plan to ensure business operation is not interrupted.
D. Run a patch management scan to discover which patches are missing from each machine.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
Which of the following should be the FIRST step to ensure an information security program meets the requirements of new regulations?
A. Validate the asset classification schema.
B. Integrate compliance into the risk management process.

C. Assess organizational security controls.
D. Conduct a gap analysis to determine necessary changes.
Answer: (SHOW ANSWER)

NEW QUESTION: 158
What should be the FIRST step when developing an asset management program?
A. Encrypt assets containing sensitive data.
B. Create a configuration management database
C. Create an asset inventory.
D. Classify assets according to risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 159
The PRIMARY goal of a post-incident review should be to
A. identify policy changes to prevent a recurrence
B. establish the cost of the incident to the business.
C. determine why the incident occurred
D. determine how to improve the incident handling process
Answer: (SHOW ANSWER)

NEW QUESTION: 160
A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's FIRST course of action?

A. Inform senior management of the new regulation.
B. Review the current security policy.
C. Determine impact to me business
D. Update the security incident management process
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
The BEST way to ensure information security efforts and initiatives continue to support corporate strategy is by:
A. including information security metrics in the organizational metrics.
B. performing periodic internal audits of the information security program
C. conducting benchmarking with industry best practices.
D. including the CIO in the information security steering committee.
Answer: (SHOW ANSWER)

NEW QUESTION: 162
Which of the following is the MOST important criterion for complete closure of a security incident?

A. Level of potential impact
B. Root cause analysis and lessons learned
C. Documenting and reporting to senior management
D. Identification of affected resources
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Information security policies should be designed PRIMARILY on the basis of:
A. international standards.
B. inherent risks.
C. business risks.
D. business demands.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
An executive's personal mobile device used for business purposes is reported lost. The information security manager should respond based on:
A. incident classification.
B. mobile device configuration.
C. the business impact analysis (BIA).
D. asset management guidelines.
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Which of the following is MOST important to have in place to help secure ongoing funding for the information security program?
A. Security balanced scorecard
B. Threat assessment repot
C. Information security strategy
D. Information security risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 166
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. System administrator
B. The business owner
C. Key customers
D. Executive management
Answer: (SHOW ANSWER)

NEW QUESTION: 167
Which of the following would be of GREATEST concern to an information security manager when evaluating a cloud service provider (CSP)?
A. Service level agreements (SLAs) art not well defined.
B. There is no right to audit the security of the provider
C. Security controls offered by the provider are inadequate
D. Data retention policies may be violated.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which of the following is an indicator of improvement in the ability to identify security risks?
A. Increased number of security audit issues resolved
B. Decreased number of information security risk assessments
C. Decreased number of staff requiring information security training
D. Increased number of reported security incidents
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
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. Unauthorized changes in the environment
C. Information security related changes
D. Information security incidents caused due to unauthorized changes
Answer: (SHOW ANSWER)

NEW QUESTION: 170
In the development of an information security strategy, recovery time objectives (RTOs) will serve as indicators of:

A. risk tolerances.
B. maturity levels.

C. senior management support.
D. open vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
When determining an acceptable risk level, which of the following is the MOST important consideration?
A. Vulnerability scores
B. System criticality
C. Threat profile
D. Risk matrices
Answer: (SHOW ANSWER)

NEW QUESTION: 172
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. Include historical data of reported incidents.
B. Provide an analysis of current risk exposures.
C. Provide the estimated return on investment (ROI)
D. include industry benchmarking comparisons.
Answer: (SHOW ANSWER)

NEW QUESTION: 173
Which of the following should be reviewed to obtain a structured overview of relevant information about an information security investment?
A. Quantitative risk analysis report
B. Information security strategy
C. Security balanced scorecard
D. Business case
Answer: (SHOW ANSWER)

NEW QUESTION: 174
What is the PRIMARY benefit to executive management when audit risk, and security functions are aligned?
A. More efficient incident handling
B. Reduced number of assurance reports
C. More effective decision making
D. More timely risk reporting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 175
When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?
A. The business continuity plan (BCP)
B. Vulnerability assessment results
C. Recommendations from senior management
D. Business impact analysis (BIA) results
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Which of the following should an information security manager do FIRST after learning about a new regulation that affects the organization?
A. Assess the noncompliance risk.
B. Notify the affected business units.
C. Inform senior management of the new regulation.
D. Evaluate the changes with legal counsel.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Which of the following defines the minimum security requirements that a specific system must meet?
A. Security policy
B. Security baseline
C. Security guideline
D. Security procedure
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which of the following should be done FIRST when establishing security measures for personal data stored and processed on a human resources....system?
A. Conduct a vulnerability assessment.
B. Conduct a privacy impact assessment (PIA).
C. Evaluate data encryption technologies.
D. Move the system into a separate network.
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Which of the following is MOST effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application?
A. Change management controls
B. Version control

C. A patch management process
D. Logical access controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 180
Which of the following is the MOST effective method to prevent a SQL injection in an employee portal?
A. Conduct network penetration testing.
B. Reconfigure the database schema.
C. Enforce referential integrity on the database.
D. Conduct code reviews.
Answer: (SHOW ANSWER)

NEW QUESTION: 181
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. Increasing security and operational staffing to support the technology
C. Restricting the use of the technology in departments with sensitive information
D. Enforcing encryption of chat communications
Answer: (SHOW ANSWER)

NEW QUESTION: 182
An incident was detected where customer records were altered without authorization. The GREATEST concern for forensic analysis would be that the log data:
A. has been disclosed.
B. could be temporarily available.
C. may be modified.
D. may not be time-synchronized.
Answer: (SHOW ANSWER)

NEW QUESTION: 183

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

NEW QUESTION: 184
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. A reduction in operational costs
C. The consolidation of tools into a single console
D. The elimination of false positive detections
Answer: (SHOW ANSWER)

NEW QUESTION: 185
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. Evaluate the cost of remediating the vulnerability
B. Report the breach of the other organization to senior management
C. Develop best and worst case scenarios
D. Reassess the risk in terms of likelihood and impact
Answer: (SHOW ANSWER)

NEW QUESTION: 186
When supporting an organization's privacy officer, which of the following is the information security managers PRIMARY role regarding privacy requirements?
A. Conducting privacy awareness programs
B. Determining data classification
C. Ensuring appropriate controls are in place
D. Monitoring the transfer of private data
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

A. Warm
B. Mobile
C. Shared
D. Redundant
Answer: (SHOW ANSWER)

NEW QUESTION: 188
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. Employee access
B. Systems configurations
C. Number of subscribers
D. Audit tights
Answer: (SHOW ANSWER)

NEW QUESTION: 189
An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification foi granting an exception to the policy?
A. USB storage devices are enabled based on user roles
B. The benefit is greater than the potential risk
C. Access is restricted to read-only.
D. Users accept the risk of noncompliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 190
A business impact analysis (BIA) should be periodically executed PRIMARILY to:
A. analyze the importance of assets.
B. verify the effectiveness of controls
C. check compliance with regulations.
D. validate vulnerabilities on environmental changes.
Answer: (SHOW ANSWER)

NEW QUESTION: 191
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: 192
When establishing the trigger levels for an organization's key risk indicators (KRIs), the thresholds should be based PRIMARILY on the organization's:
A. risk response capability.
B. current threat level.
C. risk register.
D. risk appetite.
Answer: (SHOW ANSWER)

NEW QUESTION: 193
Which of the following is MOST relevant for an information security manager to communicate to IT operations?
A. The level of exposure
B. Threat assessments
C. Vulnerability assessments
D. The level of inherent risk
Answer: (SHOW ANSWER)

NEW QUESTION: 194
Which of the following would MOST effectively help to restrict sensitive data from being transmitted outside the organization?
A. Data forensics
B. Data loss prevention (DLP)
C. Security information and event management (SIEM)
D. Intrusion detection system (IDS)
Answer: (SHOW ANSWER)

NEW QUESTION: 195
After a server has been attacked, which of the following is the BEST course of action?
A. Review vulnerability assessment
B. Initiate modem response
C. Conduct a security audit
D. Isolate the system.
Answer: (SHOW ANSWER)

NEW QUESTION: 196
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. recommend compensating controls
C. review existing technical controls.
D. document the risk exception
Answer: (SHOW ANSWER)

NEW QUESTION: 197
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. Industry best practice benchmarking results
C. Information security-related metrics
D. Identified risks and mitigating controls
Answer: (SHOW ANSWER)

NEW QUESTION: 198
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 reported social engineering attempts
C. A decrease in number of account lockouts
D. An increase in the number of viruses detected in incoming email
Answer: (SHOW ANSWER)

NEW QUESTION: 199
Which of the following is the MOST important reason for performing a cost-benefit analysis when implementing a security control?
A. To ensure that the mitigation effort does not exceed the asset value
B. To justify information security program activities
C. To present a realistic information security budget
D. To ensure that benefits are aligned with business strategies
Answer: (SHOW ANSWER)

NEW QUESTION: 200

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

A. Perform a risk assessment and share results with employees.
B. Report the findings to senior management with recommendations.
C. Include regular phishing campaigns after each training session.
D. Make the training program mandatory and enforce sanctions for noncompliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 201

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

NEW QUESTION: 202

If the inherent risk of a business activity is higher than the acceptable risk level, the information security manager should FIRST
A. recommend that management avoids the business activity
B. assess the gap between current and acceptable level of risk
C. transfer risk to a third party to avoid cost of impact
D. implement controls to mitigate the risk to an acceptable level
Answer: (SHOW ANSWER)

NEW QUESTION: 203

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

NEW QUESTION: 204

An information security manager has been asked to integrate security into the software development life cycle (SDLC) after requirements have already been gathered. In this situation during which phase would integration be MOST effectrve?
A. User acceptance testing
B. Quality assurance analysis
C. Code review
D. Penetration testing
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Which of the following is the BEST way to sustain employee interest in information security awareness in an organization?
A. Using a variety of delivery methods
B. Ensuring a common security awareness program for all staff
C. Relating security awareness programs to security policies
D. Ensuring all staff are involved
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which of the following is the MOST important outcome of testing incident response plans?
A. Internal procedures are improved.
B. An action plan is available for senior management.
C. Areas requiring investment are identified.
D. Staff is educated about current threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following BEST enables an effective escalation process within an incident response program?
A. Adequate incident response staffing
B. Monitored program metrics
C. Dedicated funding for incident management
D. Defined incident thresholds
Answer: (SHOW ANSWER)

NEW QUESTION: 208
When drafting the corporate privacy statement for a public web site, which of the following MUST be included?
A. Limited liability clause
B. Information encryption requirements
C. Explanation of information usage

D. Access control requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Which of the following activities would BEST incorporate security into the software development life cycle
{SOLO7
A. Scan operating systems for vulnerabilities
B. Minimize the use of open source software
C. Include security training for the development team
D. Test applications before go-live
Answer: (SHOW ANSWER)

NEW QUESTION: 210
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. Conduct a risk assessment
C. Interview senior management
D. Conduct a cost-benefit analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 211
During the establishment of a service level agreement (SLA) with a cloud service provider, it is MOST important for the information security manager to:
A. ensure security requirements are contractually enforceable.
B. understand the cloud storage architecture in use to determine security risk.
C. set up proper communication paths with the provider.
D. update the security policy to reflect the provider's terms of service.
Answer: (SHOW ANSWER)

NEW QUESTION: 212

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

NEW QUESTION: 213
Which of the following is the MOST important security consideration when planning to use a cloud service provider in a different country?
A. Ability to logically separate client data
B. Ability to meet business resiliency requirements
C. Ability to meet service level agreements (SLAs)
D. Ability to enforce contractual obligations
Answer: (SHOW ANSWER)

NEW QUESTION: 214
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. Restrict the distribution of confidential emails.
C. Rebuild the email application
D. Arrange for an independent review.
Answer: (SHOW ANSWER)

NEW QUESTION: 215
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:
A. identify critical processes and the degree of reliance on support services.
B. document the disaster recovery process.
C. map the business process to supporting IT and other corporate resources.
D. obtain the support of executive management.
Answer: (SHOW ANSWER)

NEW QUESTION: 216
As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain an effective information security program?

A. Implement the current information security program in the acquired company.
B. Determine new factors that could influence the information security strategy.
C. Merge the two information security programs to establish continuity.
D. Ensure information security s included in any change control efforts
Answer: (SHOW ANSWER)

NEW QUESTION: 217
Following a significant change to the underlying code of an application, it is MOST important for the information security manager to:
A. update the risk assessment.
B. validate the user acceptance testing (UAT).
C. inform senior management.
D. modify key risk indicators (KRIs).
Answer: A (LEAVE A REPLY)

NEW QUESTION: 218
Which of the following is the MOST effective approach to ensure IT processes are performed in compliance with the information security policies?
A. Identifying risks in the processes and managing those risks
B. Ensuring that key controls are embedded in the processes
C. Providing information security policy training to the process owners
D. Allocating sufficient resources
Answer: (SHOW ANSWER)

NEW QUESTION: 219
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 validated using a hash algorithm.
B. The patch should be evaluated in a testing environment.
C. The patch should be applied to critical systems.
D. The patch should be deployed quickly to systems that are vulnerable.
Answer: (SHOW ANSWER)

NEW QUESTION: 220
Which of the following is MOST critical for prioritizing actions in a business continuity plan (BCP)?
A. Asset classification
B. Business process mapping
C. Risk assessment
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 221
Which of the following is the KEY outcome of conducting a post-incident review?
A. Chain of custody is maintained.
B. Risk appetite is validated.
C. Root cause is validated.
D. Compliance requirements are met.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST.
A. initiate an investigation to determine the full extent of noncompliance
B. limit access to the Internet for employees involved.
C. notify senior management that employees are reaching policy.
D. contact the employees involved to retake security awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 223
The MOST important reason that security risk assesements should be conducted frequently through an organization is because:
A. Control effectiveness may weaken.
B. Threats to the organization may change
C. Controls should be regularly tested.
D. Compliance with legal and regulatory should be reassessed.
Answer: (SHOW ANSWER)

NEW QUESTION: 224
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: (SHOW ANSWER)

NEW QUESTION: 225
Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?
A. Adverse effects on the business
B. Legal and regulatory requirements

C. Root cause analysis results
D. Availability of resources
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Which of the following is the MOST important reason to have documented security procedures and guidelines?
A. To meet regulatory compliance requirements
B. To allocate security responsibilities to staff
C. To enable standard security practices
D. To facilitate collection of security metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 227
Which of the following techniques is MOST useful when an incident response team needs to respond to external attacks on multiple corporate network devices?
A. Security event correlation analysis
B. Vulnerability assessment of network devices
C. Penetration testing of network devices
D. Endpoint baseline configuration analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 228
Which of the following BEST describes a buffer overflow?
A. A type of covert channel that captures data.
B. A program contains a hidden and unintended function that presents a security risk.
C. A function is carried out with more data than the function can handle.
D. Malicious code designed to interfere with normal operations.
Answer: (SHOW ANSWER)

NEW QUESTION: 229

Which of the following would be MOST important to include in a business case to help obtain senior management's commitment for an information security investment?

A. Reference to business policies

B. Industry best practices

C. Results of an independent audit

D. Projected business value

Answer: (SHOW ANSWER)

NEW QUESTION: 230

Which of the following is the BEST indication that an information security control is no longer relevant?

A. IT management does not support the control.

B. Following the control costs the business more than not following it.

C. Users regularly bypass or ignore the control

D. The control does not support a specific business function.

Answer: (SHOW ANSWER)

NEW QUESTION: 231

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

A. Perform a vendor due diligence review.

B. Determine the nature of information within the application.

C. Report the application to the IT department.

D. Notify senior management of the application.

Answer: (SHOW ANSWER)

NEW QUESTION: 232

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 application vulnerability review,

B. Perform an independent code review.

C. Execute regular vulnerability scans.

D. Conduct penetration testing

Answer: (SHOW ANSWER)

NEW QUESTION: 233

Reviewing which of the following would provide the GREATEST Input to the asset classification process?

A. Replacement cost of the asset

B. Sensitivity of the data

C. Compliance requirements

D. Risk assessment

Answer: (SHOW ANSWER)

NEW QUESTION: 234
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. An explanation of the potential business impact
B. An analysis of similar attacks and recommended remediation
C. A summary of the security togs illustrating the sequence of events
D. A business case for implementing stronger logical access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 235
Which of the following is MOST important to include in an information security strategy?
A. Information security organizational structures and responsibilities
B. Cost reduction techniques for information security investments
C. Current and future desired state of information security
D. Information security program needs
Answer: (SHOW ANSWER)

NEW QUESTION: 236
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. Scheduled security assessments
C. Accountability for security functions
D. Internal reporting channels
Answer: (SHOW ANSWER)

NEW QUESTION: 237
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?
A. Updating information security awareness materials
B. Providing ongoing training to the incident response team
C. Implementing a honeypot environment
D. Implementing proactive systems monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 238
Which of the following would be MOST helpful in gaming support for a business case for an Information security initiative9

A. Emphasizing threats to the organization
B. Referencing control deficiencies
C. Demonstrating organizational alignment
D. Presenting a solution comparison matrix
Answer: (SHOW ANSWER)

NEW QUESTION: 239
Which of the following is the MOST important step in risk ranking?
A. Vulnerability analysis
B. Impact assessment
C. Mitigation cost
D. Threat assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Which of the following is the BEST way to ensure that organizational security policies comply with data security regulatory requirements?

A. Align the policies to the most stringent global regulations.
B. Obtain annual sign-off from executive management.
C. Send the policies to stakeholders for review
D. Outsource compliance activities
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Which of the following activities BEST enables executive management to ensure value delivery within an information security program?
A. Assigning an information security manager to a senior management position
B. Requiring employees to undergo information security awareness training
C. Reviewing business cases for information security initiatives
D. Approving an industry-recognized information security framework
Answer: (SHOW ANSWER)

NEW QUESTION: 242
Which of the following is MOST important for an information security manager to present to senior management on a regular basis?
A. Security controls in place to prevent the threats
B. Changes to the organization's threat environment
C. Details of reported vulnerabilities
D. False positives found on the intrusion prevention system
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Senior management is concerned a security solution may not adequately protect its multiple global data centers following recent industry breaches. What should be done NEXT?
A. Require an internal audit review.
B. Perform a gap analysis.
C. Perform a risk assessment.
D. Conduct a business impact analysis (BIA).
Answer: (SHOW ANSWER)

NEW QUESTION: 244
For an organization with operations in different parts of the world, the BEST approach for ensuring that security policies do not conflict with local laws and regulations is to:
A. adopt uniform policies.
B. refer to an external global standard to avoid any regional conflict
C. make policies at a sufficiently high level, so they are globally applicable.
D. establish a hierarchy of global and local policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 245
The value of information assets relative to the organization is BEST determined by:
A. a threat assessment.
B. an asset classification.
C. a risk assessment.
D. an impact analysis.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 246
An organization s HR department would like to outsource its employee management system to a cloud-hosted solution due to features and cost savings offered. Management has identified this solution as a business need and wants to move forward. What should be the PRIMARY role of information security in this effort?
A. Ensure a security audit is performed of the service provider.

B. Ensure the service provider has the appropriate certifications.
C. Explain security issues associated with the solution to management.
D. Determine how to securely implement the solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 247
Which of the following is the BEST approach for determining the maturity level of an information security program?
A. Evaluate key performance indicators (KPIs).
B. Perform a self-assessment.
C. Engage a third-party review.
D. Review internal audit results.
Answer: (SHOW ANSWER)

NEW QUESTION: 248
Which of the following is the BEST way to improve the timely reporting of information security incidents?
A. Incorporate security procedures in help desk processes
B. Perform periodic simulations with the incident response team.
C. Regularly reassess and update the incident response plan.
D. Integrate an intrusion detection system (IDS) in the DMZ
Answer: (SHOW ANSWER)

NEW QUESTION: 249
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. Return on investment may be inconsistently reported to senior management
B. Redundant controls may be implemented across divisions.
C. Information security governance could be decentralized by division.
D. Areas of highest risk may not be adequately prioritized for treatment.
Answer: (SHOW ANSWER)

NEW QUESTION: 250
Which of the following BEST reduces the likelihood of leakage of private information via email?
A. Email encryption
B. Strong user authentication protocols
C. Prohibition on the personal use of email
D. User awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 251
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. Excessive risk exposure in one department can be absorbed by other departments.
D. Information security governance is incorporated into organizational governance.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 252
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. Assign a data classification label.
C. Determine the risk to the data.
D. Update service level agreements (SLAs).
Answer: (SHOW ANSWER)

NEW QUESTION: 253
An organization planning to contract with a cloud service provider is concerned about the risk of account hijacking at login. What is MOST important for the organization in its security requirements to address this concern?
A. Utilize multi-factor authentication
B. Create unique login credentials for each user.
C. Utilize encryption for account logins.
D. Rotate account passwords regularly.
Answer: (SHOW ANSWER)

NEW QUESTION: 254
Which of the following is the MOST reliable way to ensure network security incidents are Identified as soon as possible'
A. Collect and correlate IT Infrastructure event logs
B. Tram help desk staff to identify and prioritize security incidents
C. Install stateful inspection firewalls
D. Conduct workshops and training sessions with end users.
Answer: (SHOW ANSWER)

NEW QUESTION: 255
The MAIN reason for internal certification of web-based business applications is to ensure:

A. changes to the organizational policy framework are identified,
B. up-to-date web technology is being used.
C. compliance with industry standards-
D. compliance with organizational policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 256
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 staff needed to detect vulnerabilities
B. A decrease in the lime needed to detect vulnerabilities
C. An increase in the number of detected vulnerabilities
D. An increase in the severity of detected vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 257
Which of the following is MOST likely to be included in an enterprise information security policy?
A. Audit trail review requirements
B. Consequences of noncompliance
C. Security monitoring strategy
D. Password composition requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 258
What should an information security manager do FIRST when a service provider that stores the organization's confidential customer data experiences a breach in its data center?
A. Recommend canceling the outsourcing contract.
B. Determine the impact of the breach.
C. Apply remediation actions to counteract the breach.
D. Engage an audit of the provider's data center.
Answer: (SHOW ANSWER)

NEW QUESTION: 259
Which of the following measures BEST indicates an improvement in the information security program to stakeholders?
A. An increase in awareness training quiz pass rates
B. A reduction in reported viruses
C. A decrease in click rates during phishing simulations
D. A downward trend in reported security incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 260
Which of the following is the GREATEST benefit of information asset classification to an organization?
A. It helps to optimize the investment in protecting information assets.
B. It demonstrates the value of information assets for financial reporting.
C. It measures qualitative value of the information.
D. It helps to minimize the cost of regulatory compliance efforts
Answer: (SHOW ANSWER)

NEW QUESTION: 261
Which of the following is the BEST indicator that an organization is appropriately managing risk?
A. A penetration test does not identify any high-risk system vulnerabilities
B. Risk assessment results are within tolerance
C. The number of events reported from the intrusion detection system (IDS) has declined.
D. The number of security incident events reported by staff has increased
Answer: (SHOW ANSWER)

NEW QUESTION: 262
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. Report to senior management.
B. Implement additional controls.
C. Conduct an impact analysis.
D. Initiate incident response processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 263
Which of the following is the BEST way to measure the effectiveness of a newly implemented social engineering training program?
A. Administer quizzes upon completion of training.
B. Test end user response to simulated scenarios

C. Track the trending of reported security incidents
D. Track the trending of malware infections.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 264
Ensuring that activities performed by outsourcing providers comply with information security policies can BEST be accomplished through the use of:
A. contractual obligations.
B. Independent audits
C. service level agreements (SLAs).
D. industry standard alignment.
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Which of the following is the MOST important consideration m a bring your own device (BYOD) program to protect company data in the event of a loss?
A. The ability to classify types of devices
B. The ability to remotely locate devices
C. The ability to restrict unapproved applications
D. The ability to centrally manage devices
Answer: (SHOW ANSWER)

NEW QUESTION: 266
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: (SHOW ANSWER)

NEW QUESTION: 267
Information classification is a fundamental step in determining:
A. who has ownership of information.
B. the type of metrics that should be captured
C. whether risk analysis objectives are met.
D. the security strategy that should be used
Answer: (SHOW ANSWER)

NEW QUESTION: 268
Which of the following is BEST performed by the security department?

A. Logging unauthorized access to the operating system
B. Provisioning users to access the operating system
C. Managing user profiles for accessing the operating system
D. Approving standards for accessing the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 269
When implementing security architecture, an information security manager MUST ensure that security controls:
A. are transparent.
B. form multiple barriers against threats.
C. are communicated through security policies.
D. are the least expensive.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 270
An information security manager is developing a new information security strategy. Which of the following functions would serve as the BEST resource to review the strategy and provide guidance for business alignment?

A. The board of directors
B. The steering committee
C. Internal audit
D. The legal department
Answer: (SHOW ANSWER)

NEW QUESTION: 271
Which of the following is the MOST important reason for logging firewall activity?
A. Incident investigation
B. Auditing purposes
C. Intrusion detection
D. Firewall tuning
Answer: (SHOW ANSWER)

NEW QUESTION: 272
The success of a computer forensic investigation depends on the concept of:
A. forensic chain
B. chain of evidence.
C. chain of attack.
D. evidence of attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 273
Which of the following is MOST critical for the successful implementation of an information security strategy?
A. Ongoing commitment from senior management
B. Compliance with regulations
C. Established information security policies
D. Sizeable funding for the information security program
Answer: (SHOW ANSWER)

NEW QUESTION: 274
An organization's recent risk assessment has identified many areas of security risk, and senior management has asked for a five-minute overview of The assessment results. Which of the following is the information security manager's BEST option for presenting this information?
A. Risk register
B. BalarKed scorecard
C. Spider diagram
D. Risk heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 275
An investigation of a recent security incident determined that the root cause was negligent handling of incident alerts by system administrators. What is the BEST way for the information security manager to address this issue?
A. Provide incident response training to data owners.
B. Conduct a risk assessment and share the results with senior management.
C. Provide incident response training to data custodians.
D. Revise the incident response plan to align with business processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 276

When outsourcing sensitive data to a cloud service provider, which of the following should be the information security manager's MOST important.....

A. Data stored at the cloud service provider is not co-hosted.

B. The cloud service provider contract includes right to audit.

C. Access authorization includes biometric security verification.

D. Roles and responsibilities have been defined for the service provider.

Answer: (SHOW ANSWER)

NEW QUESTION: 277

Which of the following should be the MOST important consideration when reporting sensitive risk-related information to stakeholders?

A. Consulting with the public relations director

B. Ensuring nonrepudiation of communication

C. Customizing the communication to the audience

D. Transmitting the internal communication securely

Answer: C (LEAVE A REPLY)

NEW QUESTION: 278

Which of the following is the MOST effective preventive control?

A. Warning banners on login screens

B. Review of audit logs

C. Segregation of duties

D. Restoration of a system from backup

Answer: (SHOW ANSWER)

NEW QUESTION: 279

To gain a clear+ understanding of the impact that a new regulatory requirement will have on an organization s information security controls, an information security manager should FIRST:

A. perform a gap analysis.

B. interview senior management

C. conduct a risk assessment

D. conduct a cost-benefit analysis.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 280

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. develop a business case.

C. map the strategy to business objectives.

D, perform a cost-benefit analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 281
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 proactively address security objectives
D. To reduce security audit issues
Answer: (SHOW ANSWER)

NEW QUESTION: 282
Which of the following should be an information security managers FIRST course of action following a decision to implement a new technology?
A. Perform a business impact analysis (BIA) on the new technology.
B. Determine security controls needed to support the new technology.
C. Determine whether the new technology will comply with regulatory requirements.
D. Perform a return-on-investment (R01) analysis for the new technology.
Answer: (SHOW ANSWER)

NEW QUESTION: 283
Segregation of duties is a security control PRIMARILY used to:
A. establish dual check.
B. establish hierarchy.
C. decentralize operations.
D. limit malicious behavior.
Answer: (SHOW ANSWER)

NEW QUESTION: 284
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. Perform periodic security assessments of the contractors' activities.
B. Require annual signed agreements of adherence to security policies
C. Conduct periodic vulnerability scans of the application.
D. Include penalties for noncompliance in the contracting agreement.
Answer: (SHOW ANSWER)

NEW QUESTION: 285

The MOST likely reason to use qualitative security risk assessments instead of quantitative methods is when:
A. an organization provides services instead of hard goods.
B. a mature security program is in place.
C. available data is too subjective.
D. a security program requires independent expression of risks.
Answer: (SHOW ANSWER)

NEW QUESTION: 286
Which of the following approaches is BEST for selecting controls to minimize information security risks?
A. Risk assessment
B. Industry best practices
C. Cost-benefit analysis
D. Control-effectiveness evaluation
Answer: (SHOW ANSWER)

NEW QUESTION: 287
Which of the following is the PRIMARY objective of reporting security metrics to stakeholders?
A. To demonstrate alignment to the business strategy
B. To communicate the effectiveness of the security program
C. To identify key controls within the organization
D. To provide support for security audit activities
Answer: (SHOW ANSWER)

NEW QUESTION: 288
A risk profile supports effective security decisions PRIMARILY because it:
A. defines how to best mitigate future risks.
B. enables comparison with industry best practices.
C. describes security threats.
D. identifies priorities for risk reduction.
Answer: (SHOW ANSWER)

NEW QUESTION: 289
An organization is concerned with the risk of information leakage caused by incorrect use of personally owned smart devices by employees. What is the BEST way for the information security manager to mitigate the associated risk?
A. Require employees to sign a nondisclosure agreement
B. implement a multi-factor authentication solution.
C. Implement a mobile device management solution.
D. Document a bong-your-own-device (BYOD) policy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 290
What should an information security team do FIRST when notified by the help desk that an employee's computer has been infected with malware?

A. Use anti-malware software to clean the infected computer.
B. Isolate the computer from the network.
C. Restore the files from a secure backup.
D. Take a forensic copy of the hard drive.
Answer: (SHOW ANSWER)

NEW QUESTION: 291
What is the BEST approach for the information security manager to reduce the impact on a security program due to turnover within the security staff?
A. Recruit certified staff.
B. Revise the information security program.
C. Ensure everyone is trained in their roles.
D. Document security procedures.
Answer: (SHOW ANSWER)

NEW QUESTION: 292
Which of the following has the GREATEST impact on efforts to improve an organization's security posture?
A. Well-documented security policies and procedures
B. Supportive tone at the top regarding security
C. Regular reporting 10 senior management
D. Automation of security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 293
When an operating system is being hardened, it is MOST important for an information security manager to ensure that

A. default passwords are changed.
B. anonymous access is removed.
C. file access is restricted
D. system logs are activated.
Answer: (SHOW ANSWER)

NEW QUESTION: 294
Which of the following is the BKT approach for an information security manager when developing new information security policies?
A. Reference an industry standard.
B. Create a stakeholder nap
C. Download a policy template
D. Establish an information security governance committee
Answer: (SHOW ANSWER)

NEW QUESTION: 295
What is the MAIN reason for an organization to develop an incident response plan?
Identify training requirements for the incident response team.
Priorities treatment based on incident critically.
What is the MAIN reason for an organization to develop an incident response plan?
A. Trigger immediate recovery procedures.
B. Provide a process for notifying stakeholders of trie incident.
C. Identity training requirements for the incident response team.
D. Prioritize treatment based on incident criticality.
Answer: (SHOW ANSWER)

NEW QUESTION: 296
An information security manager terms that the root password of an external FTP server may be subject to brute force attacks. Which of the following would be the MOST appropriate way to reduce the likelihood of a successful attack?.
A. Disable access to the externally facing server.
B. Block the source IP address of the attacker.
C. Install an intrusion detection system (IDS).
D. Lock remote logon after multiple failed attempts.
Answer: (SHOW ANSWER)

NEW QUESTION: 297
The MOST important reason for an information security manager to be involved in a new software purchase initiative is to:
A. ensure the appropriate controls are considered.
B. provide input for user requirements.

C. ensure there is software escrow in place.
D. choose the software with the most control options.
Answer: (SHOW ANSWER)

NEW QUESTION: 298
During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?
A. Eradication
B. Containment
C. Review
D. Identification
Answer: (SHOW ANSWER)

NEW QUESTION: 299
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. document and report the root cause of the incidents for senior management
B. identify security program gaps or systemic weaknesses that need correction.
C. prepare properly vetted notifications regarding the incidents to external parties
D. identify who should be held accountable for the security incidents.
Answer: (SHOW ANSWER)

NEW QUESTION: 300
Which of the following is BEST determined by using technical metrics?
A. Whether security resources are adequately allocated
B. Whether controls are operating effectively.
C. How well security risk is being managed
D. How well the security strategy is aligned with organizational objectives
Answer: D (LEAVE A REPLY)

NEW QUESTION: 301
Which of the following would provide senior management with the BEST information to better understand the organization's information security risk profile?
A. Scenarios that impact business goals
B. Scenarios that have a monetary impact
C. Scenarios that impact business operations
D. Scenarios that disrupt client services
Answer: A (LEAVE A REPLY)

NEW QUESTION: 302
Which of the following is MOST effective in the strategic alignment of security initiatives?
A. Business leaders participate in information security decision making
B. Policies are created with input from business unit managers.
C. Key information security policy are updated on a regular basis
D. A security steering committee is set up within the IT deployment.
Answer: (SHOW ANSWER)

NEW QUESTION: 303
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 key business risks
D. Identifying the threat environment
Answer: (SHOW ANSWER)

NEW QUESTION: 304
Which of the following should be of MOST influence to an information security manager when developing IT security policies?
A. IT security framework
B. Compliance with regulations
C. Business strategy
D. Put and current threats
Answer: (SHOW ANSWER)

NEW QUESTION: 305
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. Reply asking for more details.
B. Determine whether the attack is in progress.
C. Validate the authenticity of the alert.
D. Alert the network operations center
Answer: (SHOW ANSWER)

NEW QUESTION: 306
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. Slow the pace of the project to spread costs over a longer period.
C. Eliminate some of the controls from the project scope.
D. Discontinue the project to release funds for other efforts
Answer: (SHOW ANSWER)

NEW QUESTION: 307
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. Adopt a recognized framework with metrics.
C. Effective security eliminates risk to the business.
D. Security is a business product and not a process.
Answer: (SHOW ANSWER)

NEW QUESTION: 308
Which of the following is the MOST important consideration when updating procedures for managing security devices?
A. Notification to management of the procedural changes
B. Updates based on changes in risk, technology, and process
C. Review and approval of procedures by management
D. Updates based on the organization's security framework
Answer: (SHOW ANSWER)

NEW QUESTION: 309
An IT department has given a vendor remote access to the internal network for troubleshooting network performance problems. After discovering the remote activity during a firewall log review, which of the following is the FIRST course of action for an information security manager?
A. Review the related service level agreement (SLA).
B. Declare a security incident.
C. Revoke the access.
D. Determine the level of access granted
Answer: (SHOW ANSWER)

NEW QUESTION: 310

Which of the following external entities would provide the BEST guideance to an organization facing advanced attacks?

A. Disaster recovery consultants widely endorsed in industry forums
B. Open-source reconnaissance
C. Incident response experts from highly regarded peer organizations
D. Recognised threat intelligence communities
Answer: (SHOW ANSWER)

NEW QUESTION: 311
What should an information security manager do NEXT when management does not accept control recommendations resulting from a risk assessment?
A. Remove the recommendations.
B. Implement the recommendations.
C. Perform a reassessment.
D. Document the decision.
Answer: (SHOW ANSWER)

NEW QUESTION: 312
Which of the following processes is the FIRST step in establishing an information security policy?
A. Information security audit
B. Business risk assessment
C. Security controls evaluation
D. Review of current global standards
Answer: (SHOW ANSWER)

NEW QUESTION: 313
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: (SHOW ANSWER)

NEW QUESTION: 314
An organization has determined that one of its web servers has been compromised. Which of the following actions should be taken to preserve the evidence of the intrusion for forensic analysis and potential litigation?
A. Reboot the server in a secure area to search for digital evidence.
B. Restrict physical and logical access to the server.
C. Unplug the server from the power.

D. Run analysis tools to detect the source of the intrusion.
Answer: (SHOW ANSWER)

NEW QUESTION: 315
Which of the following is the MOST important consideration when establishing an information security governance framework?
A. Executive management support is obtained
B. Security steering committee meetings are held at least monthly
C. Business unit management acceptance is obtained
D. Members of the security steering committee are trained in information security.
Answer: (SHOW ANSWER)

NEW QUESTION: 316
An organization s senior management wants to allow employees to access an internal application using their personal mobile devices. Which of the following should be the information security managers FIRST course of action?
A. Assess the security risk
B. Develop a personal device policy
C. Require device encryption
D. Conduct security testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 317
The BEST way to avoid session hijacking is to use:
A. a reverse lookup.
B. a firewall
C. strong password controls.
D. a secure protocol.
Answer: (SHOW ANSWER)

NEW QUESTION: 318
Which of the following is the MOST important reason for performing a risk analysis?

A. Promoting increased security awareness in the organization
B. Identifying critical information assets
C. Identifying and eliminating threats
D. Assigning the appropriate level of protection
Answer: (SHOW ANSWER)

NEW QUESTION: 319
An organization recently rolled out a new procurement program that does not include any security requirements. Which of the following should the information security manager do FIRST?
A. Conduct security assessments of vendors based on value of annual spend with each vendor.
B. Escalate the procurement program gaps to the compliance department in case of noncompliance issues.
C. Ask internal audit to conduct an assessment of the current state of third-party security controls.
D. Meet with the head of procurement to discuss aligning security with the organization's operational objectives.
Answer: (SHOW ANSWER)

NEW QUESTION: 320
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. Important security controls may be missed without senior management input.
B. The mitigation measures may not be updated in a timely manner.
C. The security program may not be aligned with organizational objectives.
D. The cost of control implementation may be too high.
Answer: (SHOW ANSWER)

NEW QUESTION: 321
Which of the following is the BEST mechanism to prevent data loss in the event personal computing equipment is stolen or lost?
A. Personal firewall
B. Data encryption
C. Data leakage prevention (DLP)
D. Remote access to device
Answer: (SHOW ANSWER)

NEW QUESTION: 322
The PRIMARY purpose of a security information and event management (SIEM) system is to:
A. provide status of incidents
B. identify potential incidents.
C. track ongoing incidents
D. resolve incidents

Answer: B (LEAVE A REPLY)

NEW QUESTION: 323
Which of the following is the BEST way to prevent segregation of duties violations?
A. Implement role-based access.
B. Implement an identity management system.
C. Review access logs for violations.
D. Enable data encryption with strong keys.
Answer: (SHOW ANSWER)

NEW QUESTION: 324
Which of the following is the BEST way to determine if an organization's current risk level is within the risk appetite?
A. Implementing key risk indicators (KRIs)
B. Developing additional mitigating controls
C. Implementing key performance indicators (KPIs)
D. Conducting a business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 325
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. Board members are committed to the information security program
C. The information security program is continually monitored.
D. The CIO is accountable for the information security program.
Answer: (SHOW ANSWER)

NEW QUESTION: 326
Which of the following is MOST important to building an effective information security program?
A. Management support for information security
B. Information security architecture to increase monitoring activities
C. logical access controls for information systems
D. Relevant and timely content included in awareness programs
Answer: (SHOW ANSWER)

NEW QUESTION: 327
Which of the following is the BEST evidence that information security governance works as a business enabler?
A. Security key performance indicators (KPIs) are included in management briefings.
B. Business initiatives are prioritized over security initiatives.

C. Business initiatives are within risk tolerance.
D. Security initiatives have positive return on investment (ROI).
Answer: (SHOW ANSWER)

NEW QUESTION: 328
Which of the following is the BEST resource for evaluating the strengths and weaknesses of an incident response plan?
A. Incident response maturity assessment
B. Documentation from preparedness tests
C. Recovery time objectives (RTOs)
D. Mission, goals and objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 329
Which of the following needs to be established between an IT service provider and its clients to BEST enable adequate continuity of service in preparation for an outage?
A. Recovery time objectives (RTOs)
B. Data retention policies
C. Server maintenance plans
D. Reciprocal site agreement
Answer: (SHOW ANSWER)

NEW QUESTION: 330
Which of the following is the BEST approach when using sensitive customer data during the testing phase of a systems development project?

A. Sanitize customer data.
B. Implement equivalent controls to those on the source system
C. Establish the test environment on a separate network.
D. Monitor the test environment for data loss.
Answer: (SHOW ANSWER)

NEW QUESTION: 331
To integrate security into system development fie cycle (SDLC) processes, an organization MUST ensure that security.
A. Is a represented on the configuration control board.
B. Performance metrics have been met.
C. Roles and responsibly have been defined
D. Is a prerequisite for complete of major phases
Answer: (SHOW ANSWER)

NEW QUESTION: 332
Which of the following will BEST facilitate the development of appropriate incident response procedures?
A. Analyzing key risk indicators (KRIs)
B. Assessing capability maturity
C. Conducting scenario testing
D. Performing vulnerability assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 333
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: 334
Which of the following would provide the BEST justification for a new information security investment?
A. Projected reduction in risk
B. Senior management involvement in project prioritization
C. Defined key performance indicators (KPIs)
D. Results of a comprehensive threat analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 335
In an organization with effective IT risk management, the PRIMARY reason to establish key risk indicators (KRIs) is to:
A. demonstrate the alignment of risk management efforts.
B. map potential risk to key organizational strategic initiatives.
C. provide information to remediate risk events.

D. identify triggers that exceed risk thresholds
Answer: D (LEAVE A REPLY)

NEW QUESTION: 336
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. Modify the policy to accommodate the application capabilities.
C. Accept the risk and document the exception.
D. Investigate alternative mobile applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 337
Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?
A. IT strategy
B. Recovery strategy
C. Security strategy
D. Risk mitigation strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 338
Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?
A. Obtain senior management sign-off.
B. Leverage security steering committee contribution.
C. Conduct an organization-wide security audit.
D. Integrate industry best practices.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 339
Using which of the following metrics will BEST help to determine the resiliency of IT infrastructure security controls?
A. Percentage of outstanding high-risk audit issues
B. Frequency of updates to system software
C. Number of successful disaster recovery tests
D. Number of incidents resulting in disruptions
Answer: (SHOW ANSWER)

NEW QUESTION: 340
Which of the following is the MOST important requirement for the successful implementation of security governance?

A. Mapping to organizational strategies
B. Performing an enterprise-wide risk assessment
C. Aligning to an international security framework
D. Implementing a security balanced scorecard
Answer: (SHOW ANSWER)

NEW QUESTION: 341
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. Assess the possible impact
B. Isolate the breached database.
C. Implement mitigating controls.
D. Notify law enforcement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 342
When developing a classification method for incidents, the categories MUST be:
A. regularly reviewed.
B. assigned to incident handlers.
C. specific to situations.
D. quantitatively defined.
Answer: (SHOW ANSWER)

NEW QUESTION: 343
The use of digital signatures ensures that a message:
A. is not altered during transmission.
B. sender obtains acknowledgment of delivery
C. remains available during transmission
D. is not intercepted during transmission
Answer: (SHOW ANSWER)

NEW QUESTION: 344
Which of the following should be the PRIMARY consideration when developing a security governance framework for an enterprise?
A. Benchmarking against industry best practice
B. Understanding of the current business strategy
C. Assessment of the current security architecture
D. Results of a business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 345
Which of the following is the BEST advantage of a centralized information security organizational structure?
A. It is easier to manage and control business unit security teams.
B. It is more responsive to business unit needs.
C. It provides a faster turnaround for security waiver requests.
D. It allows for a common level of assurance across The enterprise.
Answer: (SHOW ANSWER)

NEW QUESTION: 346
After logging in to a web application, additional authentication is required at various application points. Which of the following is the PRIMARY reason for such an approach?
A. To meet single sign-on authentication standards
B. To support strong two-factor authentication protocols
C. To implement a challenge response test
D. To ensure access rights meet classification requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 347
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: 348
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 due diligence
C. During contract negotiations

D. During integration planning
Answer: (SHOW ANSWER)

NEW QUESTION: 349
A validated patch to address a new vulnerability that may affect a mission-critical server has been released.
What should be done immediately?
A. Add mitigating controls.
B. Check the server s security and install the patch.
C. Conduct an impact analysis.
D. Take the server off-line and install the patch.
Answer: (SHOW ANSWER)

NEW QUESTION: 350
What is the PRIMARY role of the information security program?
A. To provide guidance in managing organizational security risk
B. To perform periodic risk assessments and business impact analyses (BIAs)
C. To develop and enforce a set of security policies aligned with the business
D. To educate stakeholders regarding information security requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 351
Which of the following is MOST important to consider when defining control objectives?
A. Control recommendations from a recent audit
B. The organization's risk appetite
C. The organization's strategic objectives
D. The current level of residual risk
Answer: (SHOW ANSWER)

NEW QUESTION: 352
What should an Information security manager do FIRST to ensure an organization's security policies remain relevant for a cloud adoption?
A. Implement a cloud security policy.
B. Notify senior management of potential exposure.
C. Conduct a gap analysis
D. Include policy updates in the change control process.
Answer: (SHOW ANSWER)

NEW QUESTION: 353

A review of a number of recent XT system rollouts identified a failure to incorporate security within planning, development and implementation. Which of the following is the MOST effective way to prevent a recurrence for future systems?

A. Implement security assessments throughout the systems development life cycle.

B. Conduct regular security audits during system implementation stages.

C. Require penetration tests before production implementation.

D. Train and test system developers m secure coding practices.

Answer: (SHOW ANSWER)

NEW QUESTION: 354

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. Maintaining chain of custody

C. Determining the classification of stored data

D. Identifying the relevant strain of malware

Answer: (SHOW ANSWER)

NEW QUESTION: 355

What is the PRIMARY purpose of communicating business impact to an incident response team?

A. To enable effective prioritization of incidents

B. To facilitate resource allocation tor preventive measures

C. To provide monetary values for post-incident review

D. To provide information for communication of incidents

Answer: (SHOW ANSWER)

NEW QUESTION: 356

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: (SHOW ANSWER)

NEW QUESTION: 357

Which of the following would BEST enhance firewall security?

A. Logging of security events

B. Placing the firewall on a screened subnet

C. Providing dynamic address assignment

D. Implementing change-control practices

Answer: (SHOW ANSWER)

NEW QUESTION: 358
Which of the following is the FIRST step when defining and prioritizing security controls to be implemented under an information security program?
A. Understand the company's risk appetite and its alignment with the information security strategy
B. Review recent information security incidents to determine organizational focus areas and priorities
C. Review the applicable regulations tn place and their impact to each business function
D. Interview function owners across the company to determine the best plan of action.
Answer: (SHOW ANSWER)

NEW QUESTION: 359
The MOST important reason to have a well-documented and tested incident response plan in place is to:
A. facilitate the escalation process
B. standardize the chain of custody procedure.
C. outline external communications
D. promote a coordinated effort
Answer: (SHOW ANSWER)

NEW QUESTION: 360
When recommending a preventive control against cross-site scripting in web applications, an information security manager is MOST likely to suggest:

A. consolidating multiple sites into a single portal.
B. using https in place of http.
C. coding standards and code review.
D. hardening of the web server s operating system.
Answer: (SHOW ANSWER)

NEW QUESTION: 361
An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?
A. The data owner
B. The information security manager
C. Internal II audit
D. The data custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 362
Which of the following would BEST demonstrate the status of an organization's information security program to the board of directors?
A. Changes to information security risks
B. The information security operations matrix
C. Results of a recent external audit
D. Information security program metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 363
Which of the following processes would BEST aid an information security manager in resolving systemic security issues?
A. Reinforced security controls
B. Root cause analysis
C. Security reviews
D. Business impact anal/sis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 364
Reviewing security objectives and ensuring the integration of security across business units is PRIMARILY the focus of the:
A. executive management
B. steering committee.
C. chief information security officer (CISO).
D. board of directors.
Answer: (SHOW ANSWER)

NEW QUESTION: 365
A risk assessment report shows that phishing attacks are an emerging threat for an organization that supports online financial services. Which of the following is the information security manager's BEST course of action?
A. Conduct corporate awareness training.
B. Implement spam protection.

C. Update antivirus software
D. Transfer risk with insurance coverage.
Answer: (SHOW ANSWER)

NEW QUESTION: 366
Which of the following is the PRIMARY reason to avoid alerting certain users of an upcoming penetration test?
A. To aid in the success of the penetration
B. To reduce the scope and duration of the test
C. To evaluate detection and response capabilities
D. To prevent exploitation by malicious parties
Answer: (SHOW ANSWER)

NEW QUESTION: 367
Which of the following provides the BEST evidence that the information security program is aligned to the business strategy?
A. Information security initiatives are directly correlated to business processes.
B. Business senior management supports the information security policies.
C. The information security team is able to provide key performance indicators (KPIs) to senior management.
D. The information security program manages risk within the business1* risk tolerance.
Answer: (SHOW ANSWER)

NEW QUESTION: 368
Which of the following is the BEST reason to initiate a reassessment of current risk?
A. A recent security incident
B. Certification requirements
C. Follow-jp to an audit report
D. Changes to security personnel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 369
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. escalation procedures
C. disaster recovery plan (DRP)
D. chain of custody.
Answer: (SHOW ANSWER)

NEW QUESTION: 370

Which of the following is the MOST important element of an effective external information security communication plan?

A. Senior management approval
B. Regulatory compliance
C. Communications director approval
D. Public relations involvement
Answer: (SHOW ANSWER)

NEW QUESTION: 371
Which of the following is MOST critical when creating an incident response plan?
A. Aligning with the risk assessment process
B. Documenting incident notification and escalation processes
C. identifying what constitutes an incident
D. identifying vulnerable data assets
Answer: (SHOW ANSWER)

NEW QUESTION: 372
Which of the following is the BEST method to obtain senior management buy-in for an information security investment?
A. Including sign-off from key stakeholders
B. Demonstrating the reduction in risk
C. Communicating the end-of-life support plan from vendor
D. Providing benchmark results from alternate vendors
Answer: (SHOW ANSWER)

NEW QUESTION: 373
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. has a limited budget for coverage.
C. does not require any telecommunications connectivity.
D. is located in close proximity to the cold she.
Answer: (SHOW ANSWER)

NEW QUESTION: 374
To integrate security into system development life cycle (SDLC) processes, an organization MUST ensure that security:
A. is a prerequisite for completion of major phases.
B. is represented on the configuration control board.
C. performance metrics have been met
D. roles and responsibilities have been defined.
Answer: (SHOW ANSWER)

NEW QUESTION: 375
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. Security policy requirements
B. Ownership of information
C. Value to the business
D. Level of protection
Answer: (SHOW ANSWER)

NEW QUESTION: 376
In a resource-restricted security program, which of the following approaches will provide the BEST use of the limited resources?
A. Risk prioritization
B. Cross-training
C. Risk avoidance
D. Threat management
Answer: (SHOW ANSWER)

NEW QUESTION: 377
An organization has an approved bring your own device (BYOD) program. Which of the following is the MOST effective method to enforce application control on personal devices?
A. Establish a mobile device acceptable use policy
B. Implement a mobile device management solution.
C. Implement a web application firewall.
D. Educate users regarding the use of approved applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 378
Which of the following is the PRIMARY objective of implementing an information security strategy?
A. To maintain adherence to information security policies

B. To manage risk to an acceptable level
C. To demonstrate compliance with legal requirements
D. To align with industry best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 379
In information security governance, the PRIMARY role of the board of directors is to ensure:
A. communication of security posture to stakeholders.
B. alignment with the strategic goals of the organization
C. approval of relevant policies and standards.
D. compliance with regulations and best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 380
Which of the following is the MOST effective method for categorizing system and data criticality during the risk assessment process?

A. Interview data custodians.
B. Interview senior management.
C. Interview members of the board.
D. Interview the asset owners.
Answer: (SHOW ANSWER)

NEW QUESTION: 381
Which of the ager to regularly report to senior management?
A. Impact of untreated risks
B. Audit reports
C. Results of penetration tests
D. Threat analysis reports
Answer: (SHOW ANSWER)

NEW QUESTION: 382
An internal security audit has reported several control weaknesses. The information security manager's BEST course of action should be to:
A. remediate the vulnerabilities.
B. assign accountability for the findings.
C. determine the effect on the risk profile.
D. present the report to the steering committee.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 383

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

NEW QUESTION: 384
Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?
A. A risk assessment on the threat of data leakage
B. An unusual upward trend in outbound email volume
C. Industry benchmark of DLP investments
D. Lack of visibility into previous data leakage incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 385
The PRIMARY focus of a training curriculum for members of an incident response team should be:
A. external corporate communication
B. technology training.
C. security awareness
D. specific role training,
Answer: (SHOW ANSWER)

NEW QUESTION: 386
Which of the following is MOST helpful in protecting against hacking attempts on the production network?
A. Intrusion prevention systems
B. Network penetration testing
C. Security information and event management (SIEM) tools
D. Decentralized honeypot networks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 387
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. IT security policy dissemination.
B. rate limiting.

C. incoming traffic filtering.
D. outgoing traffic filtering.
Answer: (SHOW ANSWER)

NEW QUESTION: 388
Which of the following security characteristics is MOST important to the protection of customer data in an online transaction system?
A. Authentication
B. Data segregation
C. Audit monitoring
D. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 389
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. Implement role-based access controls.
C. Require the use of login credentials and passwords.
D. Conduct information security awareness training.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 390
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: 391
Which of the following is the MOST important consideration when determining the approach for gaining organization-wide acceptance of an information security plan?
A. Organizational information security awareness
B. Information security roles and responsibilities
C. Mature security policy
D. Organizational culture
Answer: (SHOW ANSWER)

NEW QUESTION: 392
An information security manager is implementing controls to protect the organization's data. The FIRST step in this process should be to:
A. implement access controls.
B. monitor access to the data.
C. classify the data.
D. encrypt the data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 393
Which of the following is the MOST critical security risk to consider for a start-up company in an emerging field?
A. A lack of security policies and procedures
B. New entries into the emerging marketplace
C. Loss of Intellectual property
D. Disclosure of financial statements
Answer: (SHOW ANSWER)

NEW QUESTION: 394
Which of the following is MOST likely to drive an update to the information security strategy?
A. A new chief technology officer has been hired
B. Management has decided to implement an emerging technology.
C. A recent penetration test has uncovered a control weakness.
D. A major business application has been upgraded.
Answer: (SHOW ANSWER)

NEW QUESTION: 395
Which is MOST important when aligning security priorities with business unit strategies?
A. Business impact analysis (BIA)
B. Stakeholder feedback
C. Gap analysis
D. Risk mitigation plans
Answer: (SHOW ANSWER)

NEW QUESTION: 396
Which of the following would provide the MOST helpful information when developing a prioritized list of IT assets to protect in the event of an incident?
A. The owner of the IT asset
B. The replacement cost of the IT asset
C. The classification of the information processed by the IT asset
D. The service level agreement (SLA) for the IT asset
Answer: (SHOW ANSWER)

NEW QUESTION: 397
Which of the following is MOST important for effective communication during incident response?
A. Establishing a mean time to resolve (MTTR) metric
B. Establishing a recovery time objective (RTO)
C. Maintaining a relationship with media and law enforcement
D. Maintaining an updated contact list
Answer: (SHOW ANSWER)

NEW QUESTION: 398
The PRIMARY reason for classifying assets is to:
A. inform senior management of the organization's risk posture.
B. balance asset value and protection measures.
C. establish clear lines of authority and ownership for the asset
D. identify low-value assets with insufficient controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 399
To implement a security framework, an information security manager must FIRST develop:
A. security guidelines
B. security procedures
C. security standards.
D. a security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 400
Which of the following is the MOST important influence to the continued success of an organization's information security strategy?

A. Security processes
B. Organizational culture
C. Policy development
D. Information systems

Answer: (SHOW ANSWER)