ISACA.CISM.v2020-02-16.q100

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	100
Version:	v2020-02-16
# of views:	2007
# of Questions views:	58151
https://www.freecram.net/torrent/ISACA.CISM.v2020-02-16.q100.html	

NEW QUESTION: 1
Which of the following provides the MOST relevant evidence of incident response maturity?
A. Independent audit assessment
B. Tabletop exercise results
C. Average incident closure time
D. Red team testing results
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following would provide nonrepudiation of electronic transactions?
A. Two-factor authentication
B. Receipt acknowledgment
C. Third-party certificates
D. Periodic reaccreditations
Answer: (SHOW ANSWER)

NEW QUESTION: 3
The MOST important objective of monitoring key risk indicators (KRIs) related to information security is to:
A. meet regulatory compliance requirements.
B. reduce risk management costs
C. minimize loss from security incidents.
D. identify change m security exposures.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following is the MOST important step in risk ranking?

A. Mitigation cost
B. Vulnerability analysis
C. Impact assessment
D. Threat assessment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Which of the following would provide the MOST useful input when creating an information security program?
A. Information security budget
B. Key risk indicators (KRIs)
C. Information security strategy
D. Business case
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Before final acceptance of residual risk, what is the BEST way for an information security manager to address risk factors determined to be lower than acceptable risk levels?
A. Ask senior management to lower the acceptable risk levels.
B. Ask senior management to increase the acceptable risk levels
C. Evaluate whether an excessive level of control is being applied.
D. Implement more stringent countermeasures.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following should be the FIRST step of incident response procedures?
A. Perform a risk assessment to determine the business impact.
B. Evaluate the cause of the control failure.
C. Classify the event depending on seventy and type.
D. Identify if there is a need for additional technical assistance.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
The BEST way to obtain funding from senior management for a security awareness program is to:
A. meet regulatory requirements.
B. produce a report of organizational risks.
C. demonstrate that the program will adequately reduce risk
D. produce an impact analysis report of potential breaches.
Answer: (SHOW ANSWER)

NEW QUESTION: 9

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. Users accept the risk of noncompliance.

D. Access is restricted to read-only.

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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

A. compliance with industry regulations.

B. level of support from senior management.

C. timeliness m responding to attacks.

D. key performance indicators (KPIs).

Answer: (SHOW ANSWER)

NEW QUESTION: 11

Which of the following would BEST fulfill a board of directors' request for a concise

A. Balanced scorecard

B. Risk heat map

C. Business impact analysis

D. Risk register

Answer: (SHOW ANSWER)

NEW QUESTION: 12

Which of the following is the MOST important factor when determining the frequency of information security risk reassessment?

A. Audit findings

B. Mitigating controls

C. Risk metrics

D. Risk priority

Answer: (SHOW ANSWER)

NEW QUESTION: 13

The MAIN reason for an information security manager to monitor industry level changes in the business and FT is to:

A. update information security policies in accordance with the changes

B. evaluate the effect of the changes on the levels of residual risk.

C. change business objectives based on potential impact

D. identify changes in the risk environment
Answer: (SHOW ANSWER)

NEW QUESTION: 14
The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:
A. serve as evidence of security awareness training.
B. maintain compliance with industry best practices.
C. maintain an accurate record of users access rights
D. assign accountability for transactions made with the user's ID.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following should be the information security manager's NEXT step following senior management approval of the information security strategy?
A. Develop a security pokey.
B. Form a steering committee
C. Develop a budget
D. Perform a gap analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following should be the PRIMARY factor in prioritizing responses to a security incident?
A. Incident location
B. Asset classification
C. Cost of mitigation
D. Inherent cost of assets
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
When developing a classification method for incidents, the categories MUST be:

A. specific to situations.
B. quantitatively defined.
C. regularly reviewed.
D. assigned to incident handlers.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
For a user of commercial software downloaded from the Internet, which of the following is the MOST effective means of ensuring authenticity?
A. Digital code signing
B. Digital certificates
C. Steganography
D. Digital signatures
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following will BEST help to ensure security is addressed when developing a custom application?
A. Requiring a security assessment before implementation
B. Integrating a security audit throughout the development process
C. Conducting security training for the development staff
D. Integrating security requirements into the development process
Answer: (SHOW ANSWER)

NEW QUESTION: 20
A risk has been formally accepted and documented. Which of the following is the MOST important action for an information security manager?

A. Notify senior management and the board.
B. Re-evaluate the organization's risk appetite
C. Monitor the environment for changes
D. Update risk tolerance levels.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
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. Remove overlapping security controls
B. Create a business case appeal decision.
C. Prioritize security projects based on risk.
D. Design key risk indicators (KRIs)
Answer: (SHOW ANSWER)

NEW QUESTION: 22
A risk management program will be MOST effective when:
A. risk assessments are conducted by a third party.
B. risk appetite is sustained for a long period risk
C. business units are involved in risk assessments,
D. assessments are repeated periodically
Answer: (SHOW ANSWER)

NEW QUESTION: 23
An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?
A. Perform regular audits on the implementation of critical patches.
B. Assess the patch management process
C. Evaluate patch management training.
D. Monitor and notify IT staff of critical patches
Answer: (SHOW ANSWER)

NEW QUESTION: 24
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: 25
Which of the following is MOST important when prioritizing an information security incident?
A. Criticality of affected resources
B. Cost to contain and remediate the incident
C. Short-term impact to shareholder value
D. Organizational risk tolerance
Answer: (SHOW ANSWER)

NEW QUESTION: 26
The success of a computer forensic investigation depends on the concept of:
A. chain of attack.
B. chain of evidence.
C. forensic chain
D. evidence of attack.

Answer: (SHOW ANSWER)

NEW QUESTION: 27
In which of the following ways can an information security manager BEST ensure that security controls are adequate for supporting business goals and objectives?
A. Reviewing results of the annual company external audit
B. Enforcing strict disciplinary procedures in case of noncompliance
C. Adopting internationally accepted controls
D. Using the risk management process
Answer: (SHOW ANSWER)

NEW QUESTION: 28
What should an information security manager do NEXT when management does not accept control recommendations resulting from a risk assessment?
A. Document the decision.
B. Implement the recommendations.
C. Perform a reassessment.
D. Remove the recommendations.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following recovery approaches generally has the LOWEST periodic cost?
A. Shared contingency center
B. Redundant site
C. Reciprocal agreement
D. Cold site
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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. Appoint a business manager as head of information security
C. Establish a storing committee with representation from across the organization.
D. Promote organization-wide information security awareness campaigns.
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following BEST enables an effective escalation process within an incident response program?
A. Monitored program metrics

B. Adequate incident response staffing
C. Dedicated funding for incident management
D. Defined incident thresholds
Answer: (SHOW ANSWER)

NEW QUESTION: 32
An organization implemented a mandatory information security awareness training program a year ago. What is the BEST way to determine its effectiveness?
A. Analyze findings from previous audit reports
B. Analyze results of a social engineering test
C. Analyze results from training completion reports.
D. Analyze responses from an employee survey on training satisfaction
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Who is MOST important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data toss?
A. A penetration tester to validate the attack
B. An independent auditor for identification of control deficiencies
C. A forensics expert for evidence management
D. A damage assessment expert for calculating losses
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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. The risk profile needs to be updated
B. A benchmark analysis needs to be performed.
C. Specific monitoring controls need to be implemented
D. An external review of the risk nods to be conducted

Answer: (SHOW ANSWER)

NEW QUESTION: 35
An organization involved in e-commerce activities operating from its home country opened a new office in another country wit! stringent security laws. In this scenario, the overall security strategy should be based on:
A. risk assessment results.
B. international security standards.
C. the most stringent requirements.
D. the security organization structure
Answer: (SHOW ANSWER)

NEW QUESTION: 36
The BEST way to establish a recovery time objective (RTO) that balances cost with a realistic recovery time frame is to:
A. conduct a risk assessment
B. determine daily downtime cost.
C. perform a business impact analysis (BIA).
D. analyze cost metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Meeting which of the following security objectives BEST ensures that information is protected against unauthorized modification?
A. Integrity
B. Confidentiality
C. Availability
D. Authenticity
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which of the following is a PRIMARY objective of incident classification?
A. Reducing escalations to management
B. Increasing response efficiency
C. Enabling incident reporting
D. Complying with regulatory requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following is the MOST important incident management consideration for an organization subscribing to a cloud service?

A. Expertise of personnel providing incident response
B. Decision on the classification of cloud-hosted data
C. Implementation of a SIEM in the organization
D. An agreement on the definition of a security incident
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following would be MOST helpful in gaining support for a business case for an information security initiative?

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

NEW QUESTION: 41
Which of the following should be the PRIMARY input when defining the desired state of security within an organization?
A. Level of business impact
B. External audit results
C. Annual loss expectancy
D. Acceptable risk level
Answer: (SHOW ANSWER)

NEW QUESTION: 42
The PRIMARY goal of a post-incident review should be to
A. determine why the incident occurred
B. determine how to improve the incident handling process
C. establish the cost of the incident to the business.
D. identify policy changes to prevent a recurrence
Answer: (SHOW ANSWER)

NEW QUESTION: 43
The MOST important reason that security risk assesements should be conducted frequently through an organization is because:
A. Threats to the organization may change
B. Controls should be regularly tested.
C. Control effectiveness may weaken.
D. Compliance with legal and regulatory should be reassessed.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:
A. overall IT capacity and operational constraints,
B. efficient technical processing considerations,
C. criteria consistent with classification levels
D. established guidelines
Answer: (SHOW ANSWER)

NEW QUESTION: 45
The MOST effective control to detect fraud inside an organization's network is to:
A. implement C (IDS).
B. apply two-factor authentication
C. segregate duties
D. review access logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which of the following is the MOST important reason to document information security incidents that are reported across the organization?
A. Evaluate the security posture of the organization.
B. Support business investments in security
C. Identify unmitigated risk.
D. Prevent incident recurrence.
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which of the following should be of MOST influence to an information security manager when developing IT security policies?
A. Compliance with regulations
B. IT security framework
C. Put and current threats

D. Business strategy
Answer: (SHOW ANSWER)

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

NEW QUESTION: 49
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?
A. Determine recovery priorities.
B. Analyze vulnerabilities
C. Confirm control effectiveness
D. Define the recovery point objective (RPO).
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which is MOST important when contracting an external party to perform a penetration test?
A. Define the project scope
B. Provide network documentation.
C. Obtain approval from IT management.
D. Increase the frequency of log reviews.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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. Introduce new risk scenarios to test program effectiveness.
D. Conduct programs to promote user risk awareness
Answer: (SHOW ANSWER)

NEW QUESTION: 52
A global organization is developing an incident response team (IRT). The organization wants to keep headquarters informed of aP incidents and wants to be able to present a unified response to widely dispersed events. Which of the following IRT models BEST supports these objectives?
A. Coordinating IRT

B. Distributed IRT
C. Holistic IRT
D. Central IRT
Answer: (SHOW ANSWER)

NEW QUESTION: 53
An information security manager is concerned that executive management does not su the following is the BEST way to address this situation?
A. Demonstrate alignment of the information security function with business needs.
B. Escalate noncompliance concerns to the internal audit manager
C. Report the risk and status of the information security program to the board.
D. Revise the information security strategy to meet executive management expectations.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?
A. The ability to meet deliverables
B. The cost of the services
C. The vendor's reputation m the industry
D. The business need for the function
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following BEST indicates that an information security strategy is aligned to the business strategy?
A. An adequately funded security budget
B. A fully staffed security operations center (SOC)
C. An effective information security steering committee
D. Effective information security controls organization-wide
Answer: (SHOW ANSWER)

NEW QUESTION: 56
An organization wants to integrate information security into its human resource management processes. Which of the following should be the FWST step?
A. Evaluate the cost of information security integration
B. Assess the business objectives of the processes
C. Identify information security risk associated with the processes
D. Benchmark the processes with best practice to identify gaps.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
The BEST way to improve the effectiveness of responding to and communicating security incidents is to ensure:
A. the incident response plan is regularly tested.
B. additional staff are trained and available to assist with incident response.
C. the IT budget includes funding for SIEM tools to log incidents.
D. senior management is notified at the onset of incident response.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?
A. Lack of visibility into previous data leakage incidents
B. A risk assessment on the threat of data leakage
C. An unusual upward trend in outbound email volume
D. Industry benchmark of DLP investments
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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. Industry benchmarks
B. Implementation timeframe
C. Cost-benefit analysis
D. Cost of software
Answer: (SHOW ANSWER)

NEW QUESTION: 60
When supporting a large corporation's board of directors in the development of governance, which of the following is the PRIMARY function of the information security manager?

A. Providing advice and guidance
B. Developing a balanced scorecard
C. Gaining commitment of senior management
D. Preparing the security budget
Answer: (SHOW ANSWER)

NEW QUESTION: 61
A newly hired information security manager discovers that the cleanup of accounts for terminated employees happens only once a year. Which of the following should be the information security manager's FIRST course of action?

A. Update the security policy
B. Perform a risk assessment
C. Report the issue to senior management
D. Design and document a new process
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
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. Integrate industry best practices.
C. Leverage security steering committee contribution.
D. Conduct an organization-wide security audit.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following is the MOST effective method to prevent a SQL injection in an employee portal?
A. Conduct code reviews.
B. Enforce referential integrity on the database.
C. Reconfigure the database schema.
D. Conduct network penetration testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following would BEST enhance firewall security?
A. Implementing change-control practices
B. Placing the firewall on a screened subnet
C. Providing dynamic address assignment
D. Logging of security events
Answer: (SHOW ANSWER)

NEW QUESTION: 65
When a critical incident cannot be contained in a timely manner and the affected system needs to be taken offline, which of the following stakeholders MUST receive priority communication?
A. System administrator
B. Business process owner
C. System end-users
D. Senior management
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following is an example of a deterrent control?
A. a warning banner
B. Segregation of responsibilities
C. An intrusion detection system (IDS)
D. Periodic data restoration
Answer: (SHOW ANSWER)

NEW QUESTION: 67
What would be an information security manager's BEST course of action when notified that the implementation of some security controls is being delayed due to budget constraints?
A. Begin the risk acceptance process
B. Suggest less expensive alternative security controls.
C. Prioritize security controls based on risk.
D. Request a budget exception for the security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 68
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. Lack of formal KRI approval from IT management
B. Use of qualitative measures
C. Undefined thresholds to trigger alerts
D. Multiple KRIs for a single control process
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Which of the following control type is the FIRST consideration for aligning employee behavior with an organization's information security objectives?
A. Directive security
B. Physical security control

C. Logical access control
D. Technical security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 70
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. conduct a risk assessment
B. conduct a cost-benefit analysis.
C. interview senior management
D. perform a gap analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
For a business operating in a competitive and evolving online market, it is MOST important for a security policy to focus on:
A. defining policies for new technologies.
B. managing risks of new technologies
C. requiring accreditation for new technologies.
D. enabling adoption of new Technologies.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST"
A. Data owners
B. Application owners
C. Security operations team
D. Communications department
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?
A. Internal audit reports
B. Application security policy
C. A business case
D. Vulnerability assessment results
Answer: (SHOW ANSWER)

NEW QUESTION: 74

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

NEW QUESTION: 75
The use of a business case to obtain funding for an information security investment is MOST effective when the business case:
A. realigns information security objectives to organizational strategy,
B. articulates management s intent and information security directives in clear language.
C. relates the investment to the organization's strategic plan.
D. translates information security policies and standards into business requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
An organization has implemented an enhanced password policy for business applications which requires significantly more business resource to support clients. The BEST approach to obtain the support of business management would be to:
A. Present industry benchmarking results to business units
B. Discuss the risk and impact of security incidents if not implemented
C. Elaborate on the positive impact to information security
D. Present an analysis of the cost and benefit of the changes
Answer: (SHOW ANSWER)

NEW QUESTION: 77
With limited resources in the information security department which of the following is the BEST approach for managing security risk?
A. Prioritize security activities and report to management

B. Engage a third-party company to provide security support.
C. Hire additional information security staff.
D. Implement technical solutions to automate security management activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following BEST measures the effectiveness of an organization's information security strategy?
A. Comparison of mitigated risk to accepted risk
B. Comparison of threats to vulnerabilities
C. Comparison of residual risk to risk appetite
D. Comparison of current security budget to previous year's budget
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Which of the following is the BEST approach for determining the maturity level of an information security program?
A. Perform a self-assessment.
B. Engage a third-party review.
C. Review internal audit results.
D. Evaluate key performance indicators (KPIs).
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which of the following is the BKT approach for an information security manager when developing new information security policies?

A. Download a policy template
B. Reference an industry standard.
C. Establish an information security governance committee
D. Create a stakeholder nap
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Information classification is a fundamental step in determining:
A. whether risk analysis objectives are met.
B. the security strategy that should be used
C. who has ownership of information.
D. the type of metrics that should be captured
Answer: (SHOW ANSWER)

NEW QUESTION: 82

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

NEW QUESTION: 83
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. details of expected security metrics
B. recovery time objectives (RTOs).
C. each party s security responsibilities.
D. penalties for noncompliance with security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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. Areas of highest risk may not be adequately prioritized for treatment.
B. Information security governance could be decentralized by division.
C. Return on investment may be inconsistently reported to senior management
D. Redundant controls may be implemented across divisions.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which of the following is the MOST useful input for an information security manager when refreshing the organizations security strategy?
A. Results of a vulnerability scan
B. Results of a security pokey review
C. Results of a security risk assessment
D. Results of a red team exercise
Answer: (SHOW ANSWER)

NEW QUESTION: 86
BEST way to isolate corporate data stored on employee-owned mobile devices would be to implement:

A. device encryption,
B. a strong password policy
C. a sandbox environment
D. two-factor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?
A. A report on the maturity of controls
B. Up-to-date policy and procedures documentation
C. Results of an independent assessment
D. Existence of an industry-accepted framework
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following is a PRIMARY responsibility of an information security governance committee?
A. Approving the information security awareness training strategy
B. Reviewing the information security strategy
C. Approving the purchase of information security technologies
D. Analyzing information security policy compliance reviews
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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. Review audit logs from IT systems.
B. Activate the incident response plan
C. Assess IT system configurations
D. Perform a vulnerability assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
A risk analysis for a new system is being performed. For which of the following is business knowledge MORE important than IT knowledge?

A. Impact analysis
B. Vulnerability analysis
C. Balanced scorecard
D. Cost-benefit analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 91
After a server has been attacked, which of the following is the BEST course of action?
A. Initiate modem response
B. Isolate the system.
C. Review vulnerability assessment
D. Conduct a security audit
Answer: (SHOW ANSWER)

NEW QUESTION: 92
The MAIN reason for internal certification of web-based business applications is to ensure:
A. up-to-date web technology is being used.
B. changes to the organizational policy framework are identified,
C. compliance with organizational policies.
D. compliance with industry standards-
Answer: (SHOW ANSWER)

NEW QUESTION: 93
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. Determine new factors that could influence the information security strategy.
B. Implement the current information security program in the acquired company.
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: 94
Following a successful and well-publicized hacking incident, an organization alias plans to improve application security. Which of the following is a security project risk?
A. Resources may not be available to support the implementation.

B. A trapdoor may have been installed m the application.
C. The reputation of the organization may be damaged
D. Critical evidence may be lost.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following BEST demonstrates alignment between information security governance and corporate governance?
A. Number of vulnerabilities identified for high-risk information assets
B. Security project justifications provided in terms of business value
C. Average number of security incidents across business units
D. Mean time to resolution for enterprise-wide security incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 96
A third-party service provider is developing a mobile app for an organization's customers. Which of the following issues should be of GREATEST concern to the information security management.
A. Software escrow is not addressed in the contract
B. The contract has no requirement for secure development practices
C. SLAs after deployment are not clearly defined.
D. The mobile app s programmers are all offshore contractors.
Answer: (SHOW ANSWER)

NEW QUESTION: 97
What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?
A. Establish and measure key performance indicators (KPIs)
B. Communicate incident response procedures to staff.
C. Obtain senior management commitment
D. Test incident response procedures regularly.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What is the MOST important factor for determining prioritization of incident response?
A. The availability of specialized technical staff
B. The time to restore the impacted systems
C. Service level agreements (SLAs) pertaining to the impacted systems
D. The potential impact to the business
Answer: (SHOW ANSWER)

NEW QUESTION: 99

Which of the following is the MOST effective way to mitigate the risk of confidential data leakage to unauthorized stakeholders?

A. Require the use of login credentials and passwords.

B. Create a data classification policy.

C. Conduct information security awareness training.

D. Implement role-based access controls.

Answer: (SHOW ANSWER)

NEW QUESTION: 100

The PRIMARY benefit of integrating information security risk into enterprise risk management is to:

A. obtain senior management's commitment.

B. justify the information security budget

C. ensure timely risk mitigation.

D. provide a holistic view of risk

Answer: (SHOW ANSWER)