EC-COUNCIL.712-50.v2022-05-03.q237

Exam Code:	712-50
Exam Name:	EC-Council Certified CISO (CCISO)
Certification Provider:	EC-COUNCIL
Free Question Number:	237
Version:	v2022-05-03
# of views:	3443
# of Questions views:	2370
https://www.freepdfdumps.com/EC-COUNCIL.712-50.v2022-05-03.q237.html	

NEW QUESTION: 1
In terms of supporting a forensic investigation, it is now imperative that managers, firstresponders, etc., accomplish the following actions to the computer under investigation:
A. Secure the area and shut down the computer until investigators arrive
B. Secure the area
C. Immediately place hard drive and other components in an anti-static bag
D. Secure the area and attempt to maintain power until investigators arrive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?
A. Governance
B. Management
C. Compliance
D. Awareness
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which represents PROPER separation of duties in the corporate environment?
A. Information Security and Network teams perform two distinct functions
B. Information Security and Identity Access Management teams perform two distinct functions
C. Finance has access to Human Resources data
D. Developers and Network teams both have admin rights on servers
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 4
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
Which of the following frameworks and standards will BEST fit the organization as a baseline for their security program?
A. NIST and data breach notification laws
B. NIST and Privacy Regulations
C. ISO 27000 and Payment Card Industry Data Security Standards
D. ISO 27000 and Human resources best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.
Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time.
Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.
A. Intrusion Detection Systems (IDS)
B. Data Loss Prevention (DLP)
C. Rigorous syslog reviews
D. Security Guards posted outside the Data Center
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
The patching and monitoring of systems on a consistent schedule is required by?
A. Industry best practices
B. Audit best practices
C. Risk Management frameworks
D. Local privacy laws

Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?
A. Office of the General Counsel
B. Office of the Auditor
C. All employee and users
D. Senior Executives
Answer: (SHOW ANSWER)

NEW QUESTION: 8
SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs.
The CISO discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-facto implementation project?
A. Report the deficiency to the audit team and create process exceptions
B. Decide to accept the risk on behalf of the impacted business units
C. Determine if sufficient mitigating controls can be applied
D. Create new use cases for operational use of the solution
Answer: (SHOW ANSWER)

NEW QUESTION: 9
What is the MAIN reason for conflicts between Information Technology and Information Security programs?
A. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
B. Security governance defines technology best practices and Information Technology governance does not.
C. Technology governance defines technology policies and standards while security governance does not.
D. The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10

A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website. This type of control is considered
A. Zero-day attack mitigation
B. Corrective security control
C. Dynamic blocking control
D. Preventive detection control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
A stakeholder is a person or group:
A. That will ultimately use the system.
B. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
C. Vested in the success and/or failure of a project or initiative regardless of budget implications.
D. That has budget authority.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?
A. Poor alignment of the security program to business needs
B. A lack of executive presence within the security program
C. Poor audit support for the security program
D. This is normal since business units typically resist security requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 13
When entering into a third party vendor agreement for security services, at what point in the process is it BEST to understand and validate the security posture and compliance level of the vendor?
A. Once the vendor is on premise and before they perform security services
B. Prior to signing the agreement and before any security services are being performed
C. At the time the security services are being performed and the vendor needs access to the network
D. Once the agreement has been signed and the security vendor states that they will need access to the network
Answer: (SHOW ANSWER)

NEW QUESTION: 14

You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis.
Which of the following activities will help you in this?
A. Estimate activity duration
B. Risk mitigation
C. Quantitative analysis
D. Qualitative analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
Risk appetite is typically determined by which of the following organizational functions?
A. Audit and compliance
B. Board of Directors
C. Security
D. Business units
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
Which of the following frameworks and standards will BEST fit the organization as a baseline for their security program?
A. NIST and data breach notification laws
B. ISO 27000 and Human resources best practices
C. NIST and Privacy Regulations
D. ISO 27000 and Payment Card Industry Data Security Standards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17

Which of the following are primary concerns for management with regard to assessing internal control objectives?
A. Confidentiality, Availability, Integrity
B. Compliance, Effectiveness, Efficiency
C. Communication, Reliability, Cost
D. Confidentiality, Compliance, Cost
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 18
A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?
A. Multiple references, strong background check and industry certifications
B. College degree, audit capabilities and complex project management
C. Multiple certifications, strong technical capabilities and lengthy resume
D. Industry certifications, technical knowledge and program management skills
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:
A. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
B. Inform senior management of the risk involved.
C. Agree to work with the security officer on these shifts as a form of preventative control.
D. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?
A. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
B. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
C. Create separate controls for the business based on the types of business and functions they perform

D. Provide the business units with control mandates and schedules of audits for compliance validation

Answer: (SHOW ANSWER)

NEW QUESTION: 21

An application vulnerability assessment has identified a security flaw in an application. This is a flaw that was previously identified and remediated on a prior release of the application. Which of the following is MOST likely the reason for this recurring issue?

A. High turnover in the application development department

B. Ineffective configuration management controls

C. Lack of change management controls

D. Lack of version/source controls

Answer: D (LEAVE A REPLY)

NEW QUESTION: 22

Which of the following are the triple constraints of project management?

A. Cost, quality, and time

B. Time, quality, and scope

C. Quality, scope, and cost

D. Scope, time, and cost

Answer: D (LEAVE A REPLY)

NEW QUESTION: 23

Which of the following is a strong post designed to stop a car?

A. Fence

B. Bollard

C. Reinforced rebar

D. Gate

Answer: B (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 24

What is the difference between encryption and tokenization?

A. Encryption can be mathematically reversed to provide the original information

B. Tokenization combined with hashing is always better than encryption

C. Tokenization can be mathematically reversed to provide the original information

D. The token contains the all original information

Answer: A (LEAVE A REPLY)

NEW QUESTION: 25

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?
A. The Net Present Value (NPV) of the project is positive
B. The NPV of the project is negative
C. The ROI is lower than 10 months
D. The Return on Investment (ROI) is larger than 10 months
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
The single most important consideration to make when developing your security program, policies, and processes is:
A. Establishing your authority as the Security Executive
B. Streamlining for efficiency
C. Alignment with the business
D. Budgeting for unforeseen data compromises
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
A CISO has implemented a risk management capability within the security portfolio. Which of the following terms best describes this functionality?
A. Program
B. Service
C. Cost center
D. Portfolio
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?
A. Close and chain the door shut and send a company-wide memo banning the practice.
B. Nothing, this falls outside your area of influence.
C. Have a risk assessment performed.
D. Post a guard at the door to maintain physical security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
In defining a strategic security plan for an organization, what should a CISO first analyze?
A. Review business acquisitions for the past 3 years
B. Analyze the broader organizational strategic plan

C. Reach out to a business similar to yours and ask for their plan
D. Set goals that are difficult to attain to drive more productivity
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
What type of attack requires the least amount of technical equipment and has the highest success rate?
A. Shrink wrap attack
B. Social engineering
C. War driving
D. Operating system attacks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
This occurs when the quantity or quality of project deliverables is expanded from the original project plan.
A. Deadline extension
B. Scope creep
C. Scope modification
D. Deliverable expansion
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?
A. Security Operations
B. Internal/External Audit
C. Risk Management
D. Security Administrators
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 33
The process of creating a system which divides documents based on their security level to manage access to private data is known as
A. data classification
B. data security system
C. privacy protection
D. security coding
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?
A. Lack of a security awareness program
B. Lack of identification of technology stake holders
C. Lack of influence with leaders outside IT
D. Lack of business continuity process
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Which of the following is critical in creating a security program aligned with an organization's goals?
A. Provide clear communication of security program support requirements and audit schedules
B. Ensure security budgets enable technical acquisition and resource allocation based in internal compliance requirements
C. Develop a culture in which users, managers and IT professionals all make good decisions about information risk
D. Create security awareness programs that include clear definition of security program goals and charters
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:
A. Changing the default passwords
B. Contacting the Internet Service Provider for an IP scope
C. Getting authority to operate the system from executive management

D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to_____.
A. assign the responsibility to the information security team
B. assign the responsibility to the team responsible for the management of the controls
C. perform an independent audit of the security controls
D. create operational reports on the effectiveness of the controls.
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 38
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?
A. Monitor employee browsing and surfing habits
B. Set your firewall permissions aggressively and monitor logs regularly.
C. Develop an Information Security Awareness program
D. Conduct background checks on individuals before hiring them
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?
A. Internal/External Audit
B. Security Administrators
C. Risk Management
D. Security Operations
Answer: (SHOW ANSWER)

NEW QUESTION: 40
When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?
A. Containment
B. Eradication
C. Recovery
D. Escalation

Answer: (SHOW ANSWER)

NEW QUESTION: 41
A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?
A. A clear set of security policies and procedures that are more concept-based than controls-based
B. A complete inventory of Information Technology assets including infrastructure, networks, applications and data
C. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
The company decides to release the application without remediating the high-risk vulnerabilities.
Which of the following is the MOST likely reason for the company to release the application?
A. The company does not believe the security vulnerabilities to be real
B. The company lacks the tools to perform a vulnerability assessment
C. The company lacks a risk management process
D. The company has a high risk tolerance
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 43
When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?
A. An independent Governance, Risk and Compliance organization
B. Alignment of security goals with business goals
C. Support Legal and HR teams
D. Compliance with local privacy regulations
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed.
What can be done to ensure that security is addressed cost effectively?

A. Integrate security requirements into project inception
B. Installation of new firewalls and intrusion detection systems
C. Launch an internal awareness campaign
D. User awareness training for all employees
Answer: (SHOW ANSWER)

NEW QUESTION: 45
To get an Information Security project back on schedule, which of the following will provide the MOST help?
A. Upper management support
B. Extend work hours
C. More frequent project milestone meetings
D. Stakeholder support
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?
A. Vulnerability Assessment
B. Risk Assessment
C. Risk Management
D. System Testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
The success of the Chief Information Security Officer is MOST dependent upon:
A. favorable audit findings
B. development of relationships with organization executives
C. following the recommendations of consultants and contractors
D. raising awareness of security issues with end users
Answer: (SHOW ANSWER)

NEW QUESTION: 48
When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?
A. The data custodian
B. The project manager
C. The asset owner
D. The asset manager
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?
A. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
B. Provide the business units with control mandates and schedules of audits for compliance validation
C. Create separate controls for the business units based on the types of business and functions they perform
D. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
The amount of risk an organization is willing to accept in pursuit of its mission is known as
A. Risk acceptance
B. Risk tolerance
C. Risk mitigation
D. Risk transfer
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?
A. Comprehensive Log-Files from all servers and network devices affected during the attack
B. Uninterrupted Chain of Custody
C. Expert forensics witness
D. Fully trained network forensic experts to analyze all data right after the attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.
Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?
A. Budget
B. Resources
C. Scope
D. Constraints
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called
A. Security certification
B. Security accreditation
C. Alignment with business practices and goals.
D. Security system analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?
A. Information Technology Infrastructure Library (ITIL)
B. Committee of Sponsoring Organizations (COSO)
C. Payment Card Industry (PCI)
D. Control Objective for Information Technology (COBIT)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability.
What do you do?
A. tell him to call the police
B. tell him to invoke the incident response process
C. tell him to analyze the problem, preserve the evidence and provide a full analysis and report.
D. tell him to shut down the server

Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
When dealing with a risk management process, asset classification is important because it will impact the overall:
A. Risk tolerance
B. Risk monitoring
C. Risk treatment
D. Threat identification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
When you develop your audit remediation plan what is the MOST important criteria?
A. To remediate half of the findings before the next audit.
B. To remediate all of the findings before the next audit.
C. To validate that the cost of the remediation is less than the risk of the finding.
D. To validate the remediation process with the auditor.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
A missing/ineffective security control is identified. Which of the following should be the NEXT step?
A. Perform an audit to measure the control formally
B. Establish Key Risk Indicators
C. Escalate the issue to the IT organization
D. Perform a risk assessment to measure risk
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights.
Which of the following would be the MOST concerning?
A. Lack of notification to the public of disclosure of confidential information
B. Failure to notify police of an attempted intrusion
C. Lack of reporting of a successful denial of service attack on the network.
D. Lack of notification to the public of disclosure of confidential information
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is consider a bad practice MAINLY because

A. The IT team is not certified to perform audits
B. This represents a bad implementation of the Least Privilege principle
C. The IT team is not familiar in IT audit practices
D. This represents a conflict of interest
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
Who should be involved in the development of an internal campaign to address email phishing?
A. All employees
B. Business unit leaders, CIO, CEO
C. CFO, CEO, CIO
D. Business Unite Leaders, CISO, CIO and CEO
Answer: (SHOW ANSWER)

NEW QUESTION: 62
The Information Security Governance program MUST:
A. support user choice for Bring Your Own Device (BYOD)
B. integrate with other organizational governance processes
C. integrate with other organizational governance processes
D. show a return on investment for the organization
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
Which of the following best describes revenue?
A. Non-operating financial liabilities minus expenses
B. The true profit-making potential of an organization
C. The sum value of all assets and cash flow into the business
D. The economic benefit derived by operating a business
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.investopedia.com/terms/r/revenue.asp

NEW QUESTION: 64
Which of the following is MOST useful when developing a business case for security initiatives?
A. Cost/benefit analysis
B. Vendor management
C. Budget forecasts
D. Request for proposals
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers." What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?
A. Cite corporate policy and insist on compliance with audit findings
B. Draw from your experience and recount stories of how other companies have been compromised
C. Understand the business and focus your efforts on enabling operations securely
D. Cite compliance with laws, statutes, and regulations - explaining the financial implications for the company for non-compliance
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 66
A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?
A. Meet with audit team to determine a timeline for corrections
B. Review the recommendations and follow up to see if audit implemented the changes
C. Contract with an external audit company to conduct an unbiased audit
D. Have internal audit conduct another audit to see what has changed.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.
To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

A. Business Impact Analysis
B. Business Continuity plan
C. Security roadmap
D. Annual report to shareholders
Answer: (SHOW ANSWER)
Scenario7

NEW QUESTION: 68
When selecting a security solution with reoccurring maintenance costs after the first year, the CISO should: (choose the BEST answer)
A. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
B. Implement the solution and ask for the increased operating cost budget when it is time
C. Defer selection until the market improves and cash flow is positive
D. The CISO should cut other essential programs to ensure the new solution's continued use
Answer: (SHOW ANSWER)

NEW QUESTION: 69
A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be your first priority?
A. Meet with audit team to determine a timeline for corrections
B. Have internal audit conduct another audit to see what has changed.
C. Review the recommendations and follow up to see if audit implemented the changes
D. Contract with an external audit company to conduct an unbiased audit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
When is an application security development project complete?
A. When the application reaches the maintenance phase.
B. After one year.
C. When the application is retired.
D. When the application turned over to production.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
Security related breaches are assessed and contained through which of the following?
A. Incident response
B. The IT support team.
C. Physical security team.

D. A forensic analysis.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
The risk found after a control has been fully implemented is called:
A. Total Risk
B. Residual Risk
C. Transferred risk
D. Post implementation risk
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?
A. Test every three years to ensure that things work as planned
B. Conduct periodic tabletop exercises to refine the BC plan
C. Outsource the creation and execution of the BC plan to a third party vendor
D. Conduct a Disaster Recovery (RD) exercise every year to test the plan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 74
The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to_____.
A. assign the responsibility to the information security team
B. create operational reports on the effectiveness of the controls.
C. assign the responsibility to the team responsible for the management of the controls
D. perform an independent audit of the security controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following can the company implement in order to avoid this type of security issue in the future?
A. A audit management process
B. Network based intrusion detection systems
C. A security training program for developers
D. A risk management process
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following is a benefit of a risk-based approach to audit planning?
A. Resources are allocated to the areas of the highest concern

B. Scheduling may be performed months in advance
C. Budgets are more likely to be met by the IT audit staff
D. Staff will be exposed to a variety of technologies
Answer: A (LEAVE A REPLY)
ECCouncil 712-50 : Practice Test

NEW QUESTION: 77
A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets.
This demonstrates which of the following principles?
A. Proper organizational policy enforcement
B. Security organizational policy enforcement
C. Increased security program presence
D. Regulatory compliance effectiveness
Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
What is the main purpose of the Incident Response Team?
A. Communicate details of information security incidents
B. Ensure efficient recovery and reinstate repaired systems
C. Create effective policies detailing program activities
D. Provide current employee awareness programs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
You have implemented the new controls. What is the next step?
A. Update the audit findings report
B. Monitor the effectiveness of the controls
C. Perform a risk assessment
D. Document the process for the stakeholders
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
The FIRST step in establishing a security governance program is to?
A. Conduct a risk assessment.
B. Conduct a workshop for all end users.
C. Prepare a security budget.
D. Obtain senior level sponsorship.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
Which is the BEST solution to monitor, measure, and report changes to critical data in a system?
A. File integrity monitoring
B. Syslog
C. Application logs
D. SNMP traps
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
Which of the following international standards can be BEST used to define a Risk Management process in an organization?
A. International Organization for Standardizations - 27004 (ISO-27004)
B. National Institute for Standards and Technology 800-50 (NIST 800-50)
C. International Organization for Standardizations - 27005 (ISO-27005)
D. Payment Card Industry Data Security Standards (PCI-DSS)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83
The total cost of security controls should:
A. Be greater than the value of the information resource being protected
B. Be equal to the value of the information resource being protected
C. Should not matter, as long as the information resource is protected
D. Be less than the value of the information resource being protected
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?
A. Recovery Point Objective (RPO)
B. Disaster Recovery Plan

C. Recovery Time Objective (RTO)
D. Business Continuity Plan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?
A. The auditors have not followed proper auditing processes
B. The organization has purchased cyber insurance
C. The CIO of the organization disagrees with the finding
D. The risk tolerance of the organization permits this risk
Answer: (SHOW ANSWER)

NEW QUESTION: 86
A CISO must conduct risk assessments using a method where the Chief Financial Officer (CFO) receives impact data in financial terms to use as input to select the proper level of coverage in a new cybersecurity insurance policy.
What is the MOST effective method of risk analysis to provide the CFO with the information required?
A. Conduct a quantitative risk assessment
B. Conduct a qualitative risk assessment
C. Conduct a subjective risk assessment
D. Conduct a hybrid risk assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?
A. Risk Management
B. Security Operations
C. Security Administrators
D. Internal/External Audit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
Which of the following are not stakeholders of IT security projects?
A. Third party vendors
B. Help Desk
C. Board of directors

D. CISO
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
Which of the following illustrates an operational control process:
A. Establishing procurement standards for cloud vendors
B. Classifying an information system as part of a risk assessment
C. Conducting an audit of the configuration management process
D. Installing an appropriate fire suppression system in the data center
Answer: (SHOW ANSWER)

NEW QUESTION: 90
When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?
A. Contracting rules typically require you to have conversations with two or more groups
B. Discussing decisions with a very large group of people always provides a better outcome
C. It helps to avoid regulatory or internal compliance issues
D. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 91
A digital signature addresses which of the following concerns?
A. Unauthorized reading
B. Message alteration
C. Message copying
D. Message theft
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Which of the following should be determined while defining risk management strategies?

A. Organizational objectives and risk tolerance
B. Risk assessment criteria
C. IT architecture complexity
D. Enterprise disaster recovery plans
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
Payment Card Industry (PCI) compliance requirements are based on what criteria?
A. The duration card holder data is retained
B. The number of transactions performed per year by an organization
C. The size of the organization processing credit card data
D. The types of cardholder data retained
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress.
Two projects are over a year behind schedule and way over budget. Using the best business practices for project management, you determine that the project correctly aligns with the organization goals.
What should be verified next?
A. Budget
B. Resources
C. Constraints
D. Scope
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
Scenario: Your company has many encrypted telecommunications links for their world-wide operations.
Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
Symmetric encryption in general is preferable to asymmetric encryption when:
A. The number of unique communication links is large
B. The speed of the encryption / deciphering process is essential
C. The distance to the end node is farthest away
D. The volume of data being transmitted is small
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

B. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card

C. Educate and enforce physical security policies of the company to all the employees on a regular basis

D. Setup a mock video camera next to the special card reader adjacent to the secure door

Answer: C (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 97

What is the main purpose of the Incident Response Team?

A. Ensure efficient recovery and reinstate repaired systems

B. Communicate details of information security incidents

C. Provide effective employee awareness programs

D. Create effective policies detailing program activities

Answer: A (LEAVE A REPLY)

NEW QUESTION: 98

Scenario: Your company has many encrypted telecommunications links for their world-wide operations.

Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

Symmetric encryption in general is preferable to asymmetric encryption when:

A. The number of unique communication links is large

B. The distance to the end node is farthest away

C. The volume of data being transmitted is small

D. The speed of the encryption / deciphering process is essential

Answer: D (LEAVE A REPLY)

Explanation

NEW QUESTION: 99

A missing/ineffective security control is identified.

Which of the following should be the NEXT step?

A. Escalate the issue to the IT organization

B. Perform a risk assessment to measure risk

C. Perform an audit to measure the control formally
D. Establish Key Risk Indicators
Answer: B (LEAVE A REPLY)

NEW QUESTION: 100
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.
You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?
A. Screen potential vendor solutions
B. Verify that the cost of mitigation is less than the risk
C. Get approval from the board of directors
D. Create a risk metrics for all unmitigated risks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams.
What else should be in the reporting process?
A. Executive summary
B. Names and phone numbers of those who conducted the audit
C. Business charter
D. Penetration test agreement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
A recommended method to document the respective roles of groups and individuals for a given process is to:
A. Develop an isolinear response matrix with cost benefit analysis projections
B. Develop a telephone call tree for emergency response
C. Develop a detailed internal organization chart
D. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
What is the primary reason for performing a return on investment analysis?
A. To determine the current present value of a project
B. To determine the annual rate of loss
C. To decide between multiple vendors

D. To decide is the solution costs less than the risk it is mitigating
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 104
The ultimate goal of an IT security projects is:
A. Increase stock value
B. Implement information security policies
C. Complete security
D. Support business requirements
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?
A. Incident Response
B. Risk Assessment
C. Risk Management
D. Network Security administration
Answer: C (LEAVE A REPLY)

NEW QUESTION: 106
What is the first thing that needs to be completed in order to create a security program for your organization?
A. Business continuity plan
B. Risk assessment
C. Compliance and regulatory analysis
D. Security program budget
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?
A. Risk Acceptance
B. Risk Avoidance
C. Risk Mitigation
D. Risk Transfer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?
A. Security analysts
B. Security mangers
C. Security administrators
D. Security technicians
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase.
What does this selection indicate?
A. A high threat environment
B. A low risk tolerance environment
C. A high risk tolerance environment
D. A low vulnerability environment
Answer: (SHOW ANSWER)

NEW QUESTION: 110
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations.
What authentication method is being used?
A. Shared key
B. None
C. Asynchronous
D. Open
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
Credit card information, medical data, and government records are all examples of:

A. Communications Information
B. Bodily Information
C. Territorial Information
D. Confidential/Protected Information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?
A. Compliance management
B. Audit validation
C. Physical control testing
D. Security awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 113
The process for identifying, collecting, and producing digital information in support of legal proceedings is called
A. evidence tampering.
B. electronic review.
C. electronic discovery.
D. chain of custody.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?
A. Annually
B. Quarterly
C. Bi-annually
D. Semi-annually
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 115
An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.

What is the MOST likely reason why the sensitive data was posted?
A. Data classification was not properly performed on the assets
B. The DLP Solution was not integrated with mobile device anti-malware
C. A risk assessment was not performed after purchasing the DLP solution
D. The sensitive data was not encrypted while at rest
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following can the company implement in order to avoid this type of security issue in the future?
A. Network based intrusion detection systems
B. An audit management process
C. A risk management process
D. A security training program for developers
Answer: (SHOW ANSWER)

NEW QUESTION: 117
The process of identifying and classifying assets is typically included in the
A. Business Impact Analysis
B. Asset configuration management process
C. Disaster Recovery plan
D. Threat analysis process
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following best summarizes the primary goal of a security program?
A. Assure regulatory compliance
B. Provide security reporting to all levels of an organization
C. Create effective security awareness to employees
D. Manage risk within the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 119
An organization licenses and uses personal information for business operations, and a server containing that information has been compromised.
What kind of law would require notifying the owner or licensee of this incident?
A. Special circumstance disclosure
B. Consumer right disclosure
C. Data breach disclosure
D. Security incident disclosure
Answer: (SHOW ANSWER)

NEW QUESTION: 120
The patching and monitoring of systems on a consistent schedule is required by?
A. Industry best practices
B. Audit best practices
C. Risk Management framework
D. Local privacy laws
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 121
Which type of scan is used on the eye to measure the layer of blood vessels?
A. Signature kinetics scan
B. Retinal scan
C. Iris scan
D. Facial recognition scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 122
When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization.
Which example below is the MOST creative way to maintain a strong security posture during these difficult times?
A. Download security tools from a trusted source and deploy to production network
B. Download open source security tools from a trusted site, test, and then deploy on production network
C. Download trial versions of commercially available security tools and deploy on your production network
D. Download open source security tools and deploy them on your production network
Answer: (SHOW ANSWER)

NEW QUESTION: 123

Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?
A. Fines for regulatory non-compliance
B. Decreased security awareness
C. Improper use of information resources
D. Reduction of budget
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?
A. Asset classification
B. Information security policy
C. Data classification
D. Security regulations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 125
The newly appointed CISO of an organization is reviewing the IT security strategic plan. Which of the following is the MOST important component of the strategic plan?
A. There is integration between IT security and business staffing.
B. There is a clear definition of the IT security mission and vision.
C. There is an auditing methodology in place.
D. The plan requires return on investment for all security projects.
Answer: B (LEAVE A REPLY)
ECCouncil 712-50 : Practice Test

NEW QUESTION: 126
When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?
A. ISO 27004
B. ISO 27001
C. ITILv3
D. PRINCE2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 127
The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization's
A. Security Awareness Program.
B. Anti-Spam controls.

C. Identity and Access Management Program.
D. Risk Management Program.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding.
Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?
A. The CIO of the organization disagrees with the finding
B. The risk tolerance of the organization permits this risk
C. The organization has purchased cyber insurance
D. The auditors have not followed proper auditing processes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?
A. Risk metrics
B. Management metrics
C. Operational metrics
D. Compliance metrics
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 130
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security_____.
A. Technical control
B. Management control
C. Procedural control
D. Administrative control
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 131
A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability. What do you do?
A. tell him to invoke the incident response process

B. tell him to analyze the problem, preserve the evidence and provide a full analysis and report
C. tell him to shut down the server
D. tell him to call the police
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
What is a difference from the list below between quantitative and qualitative Risk Assessment?
A. Quantitative risk assessments result in an exact number (in monetary terms)
B. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
C. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
D. Qualitative risk assessments map to business objectives
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.
What action should you take FIRST?
A. Contract with a credit reporting company for paid monitoring services for affected customers
B. Contact your local law enforcement agency
C. Consult with other C-Level executives to develop an action plan
D. Destroy the repository of stolen data
Answer: (SHOW ANSWER)

NEW QUESTION: 134
A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets. This demonstrates which of the following principles?
A. Increased security program presence
B. Proper organizational policy enforcement
C. Regulatory compliance effectiveness

D. Security alignment to business goals
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
Which is the BEST solution to monitor, measure, and report changes to critical data in a system?
A. Application logs
B. SNMP traps
C. File integrity monitoring
D. Syslog
Answer: C (LEAVE A REPLY)

NEW QUESTION: 136
A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:
A. Change management
B. Business continuity planning
C. Security Incident Response
D. Thought leadership
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Involvement of senior management is MOST important in the development of:
A. IT security procedures.
B. IT security policies.
C. Standards and guidelines.
D. IT security implementation plans.
Answer: (SHOW ANSWER)

NEW QUESTION: 138

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?
A. Compliance with local government privacy laws
B. Adherence to local data breach notification laws
C. Compliance to Payment Card Industry (PCI) data security standards
D. International encryption restrictions
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Scenario: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.
In what phase of the response will the team extract information from the affected systems without altering original data?
A. Response
B. Follow-up
C. Recovery
D. Investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Which of the following activities results in change requests?
A. Inspection
B. Defect repair
C. Corrective actions
D. Preventive actions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 141
Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?
A. System administrator
B. Data center manager
C. Data owner
D. Network architect

Answer: A (LEAVE A REPLY)

NEW QUESTION: 142
An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:
A. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.
B. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
C. Inform senior management of the risk involved.
D. Agree to work with the security officer on these shifts as a form of preventative control.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
The total cost of security controls should:
A. Be equal to the value information resource being protected
B. Should not matter, as long as the information resource is protected
C. Be greater than the value of the information resource being protected
D. Be less than the value of the information resource being protected
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 144
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?
A. Failure to notify police of an attempted intrusion
B. Lack of notification to the public of disclosure of confidential information.
C. Lack of reporting of a successful denial of service attack on the network.
D. Lack of periodic examination of access rights
Answer: (SHOW ANSWER)

NEW QUESTION: 145
The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called_____.
A. Security accreditation
B. Security certification
C. Alignment with business practices and goals
D. Security system analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:
A. Identify information assets and the underlying systems.
B. Identify and assess the risk assessment process used by management.
C. Identify and evaluate the existing controls.
D. Disclose the threats and impacts to management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
Which of the following activities is the MAIN purpose of the risk assessment process?
A. Assigning value to each information asset
B. Classifying and organizing information assets into meaningful groups
C. Calculating the risks to which assets are exposed in their current setting
D. Creating an inventory of information assets
Answer: (SHOW ANSWER)

NEW QUESTION: 148
Which of the following BEST describes an international standard framework that is based on the security model Information Technology-Code of Practice for Information Security Management?
A. Request For Comment 2196
B. International Organization for Standardization 27001
C. National Institute of Standards and Technology Special Publication SP 800-12
D. National Institute of Standards and Technology Special Publication SP 800-26
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following BEST describes an international standard framework that is based on the security model Information Technology-Code of Practice for Information Security Management?
A. National Institute of Standards and Technology Special Publication SP 800-12
B. National Institute of Standards and Technology Special Publication SP 800-26
C. International Organization for Standardization 27001
D. Request For Comment 2196
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
What is a key policy that should be part of the information security plan?
A. Remote Access policy
B. Training policy

C. Acceptable Use policy
D. Account management policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
An information security department is required to remediate system vulnerabilities when they are discovered.
Please select the three primary remediation methods that can be used on an affected system.
A. Install software patch, configuration adjustment, Software Removal
B. Install software patch, operate system, Maintain system
C. Discover software, Remove affected software, Apply software patch
D. Software removal, install software patch, maintain system
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 152
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?
A. Scan a representative sample of systems
B. Perform the scans only during off-business hours
C. Decrease the vulnerabilities within the scan tool settings
D. Filter the scan output so only pertinent data is analyzed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 153
Which of the following represents the BEST method of ensuring security program alignment to business needs?
A. Create a comprehensive security awareness program and provide success metrics to business units

B. Ensure security implementations include business unit testing and functional validation prior to production rollout
C. Create security consortiums, such as strategic security planning groups, that include business unit participation
D. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:
A. Identify information assets and the underlying systems.
B. Disclose the threats and impacts to management.
C. Identify and evaluate existing controls.
D. Identify and assess the risk assessment process used by management.
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?
A. Fines for regulatory non-compliance
B. Reduction of budget
C. Improper use of information resources
D. Decreased security awareness
Answer: A (LEAVE A REPLY)

NEW QUESTION: 156
You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll.
Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff?
A. Configure your syslog to send SMS messages to current staff when target events are triggered.
B. Employ an assumption of breach protocol and defend only essential information resources.
C. Deploy a SEIM solution and have current staff review incidents first in the morning
D. Contract with a managed security provider and have current staff on recall for incident response
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?
A. digital rights management
B. conflict resolution
C. strong authentication
D. non-repudiation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 158
Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?
A. Vulnerability management.
B. Deception technology.
C. Segmentation controls.
D. Shadow applications.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 159
Which of the following is a symmetric encryption algorithm?
A. MD5
B. 3DES
C. RSA
D. ECC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 160
Physical security measures typically include which of the following components?
A. Strong password, Biometric, Common Access Card
B. Operational, Biometric, Physical
C. Physical, Technical, Operational
D. Technical, Strong Password, Operational
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
An organization has a number of Local Area Networks (LANs) linked to form a single Wide Area Network (WAN). Which of the following would BEST ensure network continuity?
A. Full off-site backup of every server
B. Permanent alternative routing

C. Third-party emergency repair contract
D. Pre-built servers and routers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 162
The process of identifying and classifying assets is typically included in the_____.
A. Threat analysis process
B. Asset configuration management process
C. Disaster Recovery plan
D. Business Impact Analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?
A. Implementation of business-enabling information security
B. Use within an organization to formulate security requirements and objectives
C. Use within an organization to ensure compliance with laws and regulations
D. To enable organizations that adopt it to obtain certifications
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for
A. International Compliance
B. Integrity and Availability
C. Assurance, Compliance and Availability
D. Confidentiality, Integrity and Availability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 165
Which of the following intellectual Property components is focused on maintaining brand recognition?
A. Patent
B. Trademark
C. Research Logs
D. Copyright
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
Which of the following is considered a project versus a managed process?
A. monitoring external and internal environment during incident response
B. ongoing risk assessments of routine operations
C. installation of a new firewall system
D. continuous vulnerability assessment and vulnerability repair
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
The total cost of security controls should:
A. Should not matter, as long as the information resource is protected
B. be less than the value of the information resource being protected
C. Be greater than the value of the information resource being protected
D. Be equal to the value information resource being protected
Answer: (SHOW ANSWER)

NEW QUESTION: 168
The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:
A. Due Compromise
B. Due process
C. Due Care
D. Due Protection
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 169
To have accurate and effective information security policies how often should the CISO review the organization policies?
A. Every 6 months
B. Quarterly
C. Before an audit

D. At least once a year
Answer: D (LEAVE A REPLY)
ECCouncil 712-50 : Practice Test

NEW QUESTION: 170
You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?
A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk Transfer
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 171
Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?
A. In-line hardware keyloggers are relatively inexpensive
B. In-line hardware keyloggers don't require physical access
C. In-line hardware keyloggers are undetectable by software
D. In-line hardware keyloggers don't comply to industry regulations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
Scenario: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning.
Which of the following is the MOST logical next step?
A. Report the audit findings and remediation status to business stake holders
B. Create detailed remediation funding and staffing plans
C. Review security procedures to determine if they need modified according to findings
D. Validate the effectiveness of current controls
Answer: (SHOW ANSWER)

NEW QUESTION: 173
What is the FIRST step in developing the vulnerability management program?
A. Define Policy
B. Baseline the Environment
C. Organization Vulnerability

D. Maintain and Monitor
Answer: B (LEAVE A REPLY)

NEW QUESTION: 174
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:
A. They are subjective and can be completed more quickly
B. They are objective and can express risk / cost in real numbers
C. They are objective and express risk / cost in approximates
D. They are subjective and can express risk / cost real numbers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
An example of professional unethical behavior is:
A. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation
B. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
C. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
D. Storing client lists and other sensitive corporate internal documents on a removable thumb drive
Answer: (SHOW ANSWER)

NEW QUESTION: 176
When performing a forensic investigation, what are the two MOST common data sources for obtaining evidence from a computer and mobile devices?
A. RAM and unallocated space
B. Slack space and browser cache
C. Unallocated space and RAM
D. Persistent and volatile data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 177
According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?
A. Decide how to manage risk
B. Define Information Security Policy
C. Define the budget of the Information Security Management System
D. Identify threats, risks, impacts and vulnerabilities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?
A. Security officer
B. Vulnerability engineer
C. System administrator
D. Data owner
Answer: C (LEAVE A REPLY)

NEW QUESTION: 179
One of the MAIN goals of a Business Continuity Plan is to
A. Assign responsibilities to the technical teams responsible for the recovery of all data.
B. Provide step by step plans to recover business processes in the event of a disaster
C. Ensure all infrastructure and applications are available in the event of a disaster
D. Allow all technical first-responders to understand their roles in the event of a disaster
Answer: B (LEAVE A REPLY)

NEW QUESTION: 180
Which of the following has the GREATEST impact on the implementation of an information security governance model?
A. Complexity of organizational structure
B. Distance between physical locations
C. Organizational budget
D. Number of employees
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 181
Which of the following backup sites takes the longest recovery time?
A. Cold site
B. Hot site
C. Warm site
D. Mobile backup site
Answer: A (LEAVE A REPLY)
ECCouncil 712-50 : Practice Test

NEW QUESTION: 182
Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?
A. Single loss expectancy multiplied by the annual rate of occurrence
B. Replacement cost multiplied by the single loss expectancy
C. Value of the asset multiplied by the loss expectancy
D. Total loss expectancy multiplied by the total loss frequency
Answer: A (LEAVE A REPLY)

NEW QUESTION: 183
As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand.
Which is the BEST type of risk that defines this event?
A. Compliance Risk
B. Operational Risk
C. Strategic Risk
D. Reputation Risk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following represents the best method of ensuring business unit alignment with security program requirements?
A. Create collaborative risk management approaches within the organization
B. Demonstrate executive support with written mandates for security policy adherence
C. Provide clear communication of security requirements throughout the organization
D. Perform increased audits of security processes and procedures
Answer: A (LEAVE A REPLY)

NEW QUESTION: 185
A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims.
Which of the following vendor provided documents is BEST to make your decision:
A. Vendor's client list of reputable organizations currently using their solution
B. Vendor provided reference from an existing reputable client detailing their implementation

C. Vendor provided attestation of the detailed security controls from a reputable accounting firm
D. Vendor provided internal risk assessment and security control documentation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 186
An organization information security policy serves to
A. establish acceptable systems and user behavior
B. define relationships with external law enforcement agencies
C. establish budgetary input in order to meet compliance requirements
D. define security configurations for systems
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?
A. Better understand the threats and vulnerabilities affecting the environment
B. Better understand strengths and weakness of the program
C. Meet regulatory compliance requirements
D. Meet legal requirements
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 188
A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?
A. Physical control testing
B. Security awareness training
C. Compliance management
D. Audit validation
Answer: (SHOW ANSWER)

NEW QUESTION: 189
From the CISO's perspective in looking at financial statements, the statement of retained earnings of an organization:
A. Has a direct correlation with the CISO's budget
B. Represents the percentage of earnings that could in part be used to finance future security controls
C. Represents, in part, the savings generated by the proper acquisition and implementation of security controls

D. Represents the sum of all capital expenditures
Answer: B (LEAVE A REPLY)

NEW QUESTION: 190
Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?
A. Financial reporting regulations
B. Credit card compliance and regulations
C. Local privacy laws
D. Strong authentication technologies
Answer: (SHOW ANSWER)

NEW QUESTION: 191
A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?
A. The software license expiration is probably out of synchronization with other software licenses
B. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects
C. The project was initiated without an effort to get support from impacted business units in the organization
D. The software is out of date and does not provide for a scalable solution across the enterprise
Answer: (SHOW ANSWER)

NEW QUESTION: 192
A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state. Which of the following security issues is the MOST likely reason leading to the audit findings?
A. Lack of change management processes
B. Lack of hardening standards
C. Lack of proper access controls
D. Lack of asset management processes
Answer: (SHOW ANSWER)

NEW QUESTION: 193

When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization. Which example below is the MOST creative way to maintain a strong security posture during these difficult times?
A. Download security tools from a trusted source and deploy to production network
B. Download open source security tools from a trusted site, test, and then deploy on production network
C. Download trial versions of commercially available security tools and deploy on your production network
D. Download open source security tools and deploy them on your production network
Answer: B (LEAVE A REPLY)

NEW QUESTION: 194
Which of the following statements about Encapsulating Security Payload (ESP) is true?
A. It is a text-based communication protocol.
B. It uses UDP port 22
C. It is an IPSec protocol.
D. It uses TCP port 22 as the default port and operates at the application layer.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization.
Which of the following principles does this best demonstrate?
A. Leveraging existing implementations
B. Alignment with the business
C. Effective use of existing technologies
D. Proper budget management
Answer: (SHOW ANSWER)

NEW QUESTION: 196
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?
A. Effective use of existing technologies
B. Leveraging existing implementations
C. Proper budget management
D. Alignment with the business
Answer: D (LEAVE A REPLY)

NEW QUESTION: 197
The alerting, monitoring and life-cycle management of security related events is typically handled by the_____.
A. risk management process
B. risk assessment process
C. governance, risk, and compliance tools
D. security threat and vulnerability management process
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 198
What is the FIRST step in developing the vulnerability management program?
A. Maintain and Monitor
B. Baseline the Environment
C. Define Policy
D. Organization Vulnerability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 199
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure.
What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?
A. Decrease the vulnerabilities within the scan tool settings
B. Scan a representative sample of systems
C. Filter the scan output so only pertinent data is analyzed
D. Perform the scans only during off-business hours
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 200
The rate of change in technology increases the importance of:

A. Understanding user requirements.
B. Outsourcing the IT functions.
C. Implementing and enforcing good processes.
D. Hiring personnel with leading edge skills.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?
A. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
B. A complete inventory of Information Technology assets including infrastructure, networks, applications and data
C. A clear set of security policies and procedures that are more concept-based than controls-based
D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in
Answer: D (LEAVE A REPLY)

NEW QUESTION: 202
When deploying an Intrusion Prevention System (IPS), the BEST way to get maximum protection from the system is to deploy it_____
A. In-line and turn on alert mode to stop malicious traffic.
B. In promiscuous mode and only detect malicious traffic.
C. In promiscuous mode and block malicious traffic.
D. In-line and turn on blocking mode to stop malicious traffic in-line.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 203
In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?
A. High risk environments 6 months, low-risk environments 12 months
B. Every 6 months
C. Every 12 months
D. Every 18 months
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the following best describes the sensors designed to project and detect a light beam across an area?

A. Photo electric
B. Thermal
C. Air-aspirating
D. Smoke
Answer: A (LEAVE A REPLY)

NEW QUESTION: 205
When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?
A. Risk Avoidance, Threat Level, and Consequences of Compromise
B. Reputational Impact, Financial Impact, and Risk of Compromise
C. Risk Transfer, Reputational Impact, and Consequences of Compromise
D. Threat Level, Risk of Compromise, and Consequences of Compromise
Answer: D (LEAVE A REPLY)

NEW QUESTION: 206
When reviewing a Solution as a Service (SaaS) provider's security health and posture, which key document should you review?
A. SOC-2 Report
B. Metasploit Audit Report
C. Statement from SaaS provider attesting their ability to secure your data
D. SaaS provider's website certifications and representations (certs and reps)
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Security related breaches are assessed and contained through which of the following?
A. Incident response
B. Physical security team.
C. A forensic analysis.
D. The IT support team.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 208
When selecting a security solution with reoccurring maintenance costs after the first year (choose the BEST answer):
A. Defer selection until the market improves and cash flow is positive
B. The CISO should cut other essential programs to ensure the new solution's continued use
C. Implement the solution and ask for the increased operating cost budget when it is time
D. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use

Answer: D (LEAVE A REPLY)

NEW QUESTION: 209
Risk appetite is typically determined by which of the following organizational functions?
A. Board of Directors
B. Security
C. Business units
D. Audit and compliance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 210
The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees. Which of the following can be used as a KPI?
A. Number of callers who report security issues.
B. Number of successful social engineering attempts on the call center
C. Number of callers who report a lack of customer service from the call center
D. Number of callers who abandon the call before speaking with a representative
Answer: B (LEAVE A REPLY)

NEW QUESTION: 211
Control Objectives for Information and Related Technology (COBIT) is which of the following?
A. An audit guideline for certifying secure systems and controls
B. A framework for Information Technology management and governance
C. A set of international regulations for Information Technology governance
D. An Information Security audit standard
Answer: B (LEAVE A REPLY)

NEW QUESTION: 212
Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover

that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.
To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?
A. Business Continuity plan
B. Annual report to shareholders
C. Security roadmap
D. Business Impact Analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 213
The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is
A. External Audit
B. Forensic experts
C. Internal Audit
D. Penetration testers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 214
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy.
This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?
A. Lack of a formal risk management policy
B. Lack of a formal security awareness program
C. Lack of normal definition of roles and responsibilities
D. Lack of a formal security policy governance process
Answer: (SHOW ANSWER)

NEW QUESTION: 215
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?
A. IT security centric agenda
B. Lack of risk management process
C. Compliance centric agenda

D. Lack of risk management process
Answer: A (LEAVE A REPLY)

NEW QUESTION: 216
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?
A. Failure to notify police of an attempted intrusion
B. Lack of periodic examination of access rights
C. Lack of reporting of a successful denial of service attack on the network.
D. Lack of notification to the public of disclosure of confidential information.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 217
An organization's Information Security Policy is of MOST importance because_____.
A. It defines a process to meet compliance requirements
B. It communicates management's commitment to protecting information resources
C. It establishes a framework to protect confidential information
D. It is formally acknowledged by all employees and vendors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 218
When managing the critical path of an IT security project, which of the following is MOST important?
A. Knowing who all the stakeholders are.
B. Knowing the milestones and timelines of deliverables.
C. Knowing the threats to the organization.
D. Knowing the people on the data center team.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 219
A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?
A. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
B. If the findings do not impact regulatory compliance, review current security controls.
C. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
D. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 220
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?
A. Adherence to local data breach notification laws
B. Compliance to Payment Card Industry (PCI) data security standards
C. Compliance with local government privacy laws
D. International encryption restrictions
Answer: B (LEAVE A REPLY)

NEW QUESTION: 221
A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website. This type of control is considered
A. Dynamic blocking control
B. Zero-day attack mitigation
C. Preventive detection control
D. Corrective security control
Answer: D (LEAVE A REPLY)

NEW QUESTION: 222
When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?
A. Threat Level, Risk of Compromise, and Consequences of Compromise
B. Risk Avoidance, Threat Level, and Consequences of Compromise
C. Risk Transfer, Reputational Impact, and Consequences of Compromise
D. Reputational Impact, Financial Impact, and Risk of Compromise
Answer: A (LEAVE A REPLY)
ECCouncil 712-50 : Practice Test

NEW QUESTION: 223
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security_____.
A. Administrative control
B. Management control
C. Procedural control
D. Technical control

Answer: B (LEAVE A REPLY)

NEW QUESTION: 224
A Security Operations (SecOps) Manager is considering implementing threat hunting to be able to make better decisions on protecting information and assets.
What is the MAIN goal of threat hunting to the SecOps Manager?
A. Validate patterns of behavior related to an attack
B. Enhance tuning of automated tools to detect and prevent attacks
C. Replace existing threat detection strategies
D. Improve discovery of valid detected events
Answer: D (LEAVE A REPLY)

NEW QUESTION: 225
In terms of supporting a forensic investigation, it is now imperative that managers, first-responders, etc., accomplish the following actions to the computer under investigation:
A. Secure the area and shut-down the computer until investigators arrive
B. Secure the area.
C. Immediately place hard drive and other components in an anti-static bag
D. Secure the area and attempt to maintain power until investigators arrive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 226
If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization. How would you prevent such type of attacks?
A. Conduct thorough background checks before you engage them
B. It is impossible to block these attacks
C. Hire the people through third-party job agencies who will vet them for you
D. Investigate their social networking profiles
Answer: A (LEAVE A REPLY)

NEW QUESTION: 227
A recommended method to document the respective roles of groups and individuals for a given process is to:
A. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart
B. Develop an isolinear response matrix with cost benefit analysis projections
C. Develop a detailed internal organization chart
D. Develop a telephone call tree for emergency response
Answer: A (LEAVE A REPLY)

NEW QUESTION: 228
Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of_____.
A. Network based security detective controls
B. Software segmentation controls
C. Network based security preventative controls
D. User segmentation controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:
A. NOPS
B. 'O 1=1 - -
C. "DROPTABLE USERNAME"
D. /../../../../
Answer: B (LEAVE A REPLY)

NEW QUESTION: 230
Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the incident handling process will utilize the signature to resolve this incident?
A. Eradication
B. Identification
C. Containment
D. Recovery
Answer: A (LEAVE A REPLY)

NEW QUESTION: 231

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees.
Which of the following can be used as a KPI?
A. Number of successful social engineering attempts on the call center
B. Number of callers who abandon the call before speaking with a representative
C. Number of callers who report a lack of customer service from the call center
D. Number of callers who report security issues.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 232
Which of the following best summarizes the primary goal of a security program?
A. Create effective security awareness to employees
B. Manage risk within the organization
C. Provide security reporting to all levels of an organization
D. Assure regulatory compliance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 233
Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?
A. Clear
B. Mangle
C. Destroy
D. Purge
Answer: (SHOW ANSWER)

NEW QUESTION: 234
An organization's Information Security Policy is of MOST importance because
A. it communicates management's commitment to protecting information resources
B. it is formally acknowledged by all employees and vendors
C. it defines a process to meet compliance requirements
D. it establishes a framework to protect confidential information
Answer: (SHOW ANSWER)

NEW QUESTION: 235
The process of identifying and classifying assets is typically included in the
A. Business Impact Analysis
B. Asset configuration management process
C. Threat analysis process

D. Disaster Recovery plan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
When gathering security requirements for an automated business process improvement program, which of the following is MOST important?
A. Type of data contained in the process/system
B. Type of computer the data is processed on
C. Type of encryption required for the data once it is at rest
D. Type of connection/protocol used to transfer the data
Answer: (SHOW ANSWER)

NEW QUESTION: 237
SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:
A. /../../../../
B. "DROPTABLE USERNAME"
C. ' o 1=1 - -
D. NOPS
Answer: (SHOW ANSWER)