EC-COUNCIL.712-50.v2022-09-05.q134

Exam Code:	712-50
Exam Name:	EC-Council Certified CISO (CCISO)
Certification Provider:	EC-COUNCIL
Free Question Number:	134
Version:	v2022-09-05
# of views:	1765
# of Questions views:	1340
https://www.freepdfdumps.com/EC-COUNCIL.712-50.v2022-09-05.q134.html	

NEW QUESTION: 1
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:
A. Scanning for viruses
B. Password changes
C. Baselining of computer systems
D. Controlled spear phishing campaigns
Answer: (SHOW ANSWER)

NEW QUESTION: 2
What is the FIRST step in developing the vulnerability management program?
A. Organization Vulnerability
B. Define Policy
C. Maintain and Monitor
D. Baseline the Environment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?
A. Internal Audit
B. Information Security
C. Compliance
D. Database Administration
Answer: B (LEAVE A REPLY)

Explanation

NEW QUESTION: 4
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. Audit validation
B. Physical control testing
C. Security awareness training
D. Compliance management
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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. Discussing decisions with a very large group of people always provides a better outcome
B. It helps to avoid regulatory or internal compliance issues
C. Contracting rules typically require you to have conversations with two or more groups
D. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
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. Risk Management Program.
B. Identity and Access Management Program.
C. Security Awareness Program.
D. Anti-Spam controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
An organization information security policy serves to_____.
A. define relationship with external law enforcement agencies
B. establish acceptable systems and user behavior
C. establish budgetary input in order to meet compliance requirements
D. define security configurations for systems
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8

A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company's building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted are a. Which type of attack did the consultant perform?

A. Social engineering

B. Mantrap

C. Tailgating

D. Shoulder surfing

Answer: (SHOW ANSWER)

NEW QUESTION: 9

The new CISO was informed of all the Information Security projects that the organization has in progress. Two projects are over a year behind schedule and over budget. Using best business practices for project management you determine that the project correctly aligns with the company goals.

Which of the following needs to be performed NEXT?

A. Verify the scope of the project

B. Verify the regulatory requirements

C. Verify capacity constraints

D. Verify technical resources

Answer: D (LEAVE A REPLY)

NEW QUESTION: 10

Which of the following is the MOST important goal of risk management?

A. Identifying the risk

B. Assessing the impact of potential threats

C. Finding economic balance between the impact of the risk and the cost of the control

D. Identifying the victim of any potential exploits.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 11

The Information Security Management program MUST protect:

A. critical business processes and /or revenue streams

B. intellectual property released into the public domain

C. against distributed denial of service attacks

D. all organizational assets

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12

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 attestation of the detailed security controls from a reputable accounting firm
C. Vendor provided internal risk assessment and security control documentation
D. Vendor provided reference from an existing reputable client detailing their implementation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?
A. Hardware error reports
B. Availability reports
C. Utilization reports
D. Systems logs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?
A. Risk Assessment
B. Incident Response
C. Network Security administration
D. Risk Management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
Which of the following can the company implement in order to avoid this type of security issue in the future?
A. A security training program for developers
B. A risk management process
C. Network based intrusion detection systems
D. An audit management process
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16

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.
The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization.
From an organizational perspective, which of the following is the LIKELY reason for this?
A. The CISO reports to the IT organization
B. The CISO has not implemented a policy management framework
C. The CISO does not report directly to the CEO of the organization
D. The CISO has not implemented a security awareness program
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 17
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 asset management processes
D. Lack of proper access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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.

Which of the following is the FIRST action the CISO will perform after receiving the audit report?

A. Validate gaps and accept or dispute the audit findings

B. Create remediation plans to address program gaps

C. Determine if security policies and procedures are adequate

D. Inform peer executives of the audit results

Answer: A (LEAVE A REPLY)

NEW QUESTION: 19

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 administrators

C. Security technicians

D. Security mangers

Answer: D (LEAVE A REPLY)

NEW QUESTION: 20

Which of the following is MOST likely to be discretionary?

A. Standards

B. Policies

C. Procedures

D. Guidelines

Answer: D (LEAVE A REPLY)

NEW QUESTION: 21

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. Permanent alternative routing

B. Full off-site backup of every server

C. Third-party emergency repair contract

D. Pre-built servers and routers

Answer: A (LEAVE A REPLY)

NEW QUESTION: 22

Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

A. Create separate controls for the business units based on the types of business and functions they perform

B. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data

C. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
D. Provide the business units with control mandates and schedules of audits for compliance validation
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:
A. Develop a cost-benefit analysis
B. Create timelines for mitigation
C. Create a detailed technical executive summary
D. Calculate annual loss expectancy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
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. ISO 27000 and Payment Card Industry Data Security Standards
B. NIST and data breach notification laws
C. NIST and Privacy Regulations
D. ISO 27000 and Human resources best practices
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
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. Follow-up
B. Recovery
C. Response

D. Investigation
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 26
With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:
A. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program
B. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
C. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program
Answer: (SHOW ANSWER)

NEW QUESTION: 27
You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults.
Which of the following is a default community string?
A. Public
B. Administrator
C. Execute
D. Read
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 28
An organization's Information Security Policy is of MOST importance because_____.
A. It defines a process to meet compliance requirements
B. It establishes a framework to protect confidential information
C. It communicates management's commitment to protecting information resources
D. It is formally acknowledged by all employees and vendors
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 29
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 provided internal risk assessment and security control documentation
B. Vendor's client list of reputable organizations currently using their solution
C. Vendor provided attestation of the detailed security controls from a reputable accounting firm
D. Vendor provided reference from an existing reputable client detailing their implementation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
What oversight should the information security team have in the change management process for application security?
A. Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production
B. Information security should be aware of all application changes and work with developers before changes and deployed in production
C. Information security should be informed of changes to applications only
D. Development team should tell the information security team about any application security flaws
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 31
Which wireless encryption technology makes use of temporal keys?
A. Wi-Fi Protected Access version 1 (WPA2)
B. Wireless Application Protocol (WAP)
C. Wireless Equivalence Protocol (WEP)
D. Extensible Authentication Protocol (EAP)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
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. Lack of risk management process
B. Lack of sponsorship from executive management
C. IT security centric agenda
D. Compliance centric agenda
Answer: C (LEAVE A REPLY)
Scenario9

NEW QUESTION: 33
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.
Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?
A. Upper management support
B. More frequent project milestone meetings
C. More training of staff members
D. Involve internal audit
Answer: A (LEAVE A REPLY)
Scenario10

NEW QUESTION: 34
The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?
A. Management metrics
B. Risk metrics
C. Operational metrics
D. Compliance metrics
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Which of the following is the MAIN security concern for public cloud computing?

A. Unable to control physical access to the servers
B. Unable to track log on activity
C. Unable to run anti-virus scans
D. Unable to patch systems as needed
Answer: (SHOW ANSWER)

NEW QUESTION: 36
A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?
A. An insider
B. Poorly configured firewalls
C. Malware
D. Advanced Persistent Threat (APT)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?
A. Reduction of budget
B. Improper use of information resources
C. Fines for regulatory non-compliance
D. Decreased security awareness
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
The ability to demand the implementation and management of security controls on third parties providing services to an organization is
A. Compliance management
B. Vendor management
C. Security Governance
D. Disaster recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
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 familiar in IT audit practices
B. The IT team is not certified to perform audits
C. This represents a bad implementation of the Least Privilege principle
D. This represents a conflict of interest

Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following activities must be completed BEFORE you can calculate risk?
A. Assessing the relative risk facing the organization's information assets
B. Assigning a value to each information asset
C. Determining the likelihood that vulnerable systems will be attacked by specific threats
D. Calculating the risks to which assets are exposed in their current setting
Answer: (SHOW ANSWER)

NEW QUESTION: 41
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. Discover software, Remove affected software, Apply software patch
C. Software removal, install software patch, maintain system
D. Install software patch, Operate system, Maintain system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
Which of the following is the MOST important reason for performing assessments of the security portfolio?
A. To create executive support of the portfolio
B. To assure that the portfolio is aligned to the needs of the broader organization
C. To discover new technologies and processes for implementation within the portfolio
D. To provide independent 3rd party reviews of security effectiveness
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is
A. Penetration testers
B. External Audit
C. Forensic experts
D. Internal Audit
Answer: (SHOW ANSWER)

NEW QUESTION: 44

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 lacks the tools to perform a vulnerability assessment

B. The company does not believe the security vulnerabilities to be real

C. The company lacks a risk management process

D. The company has a high risk tolerance

Answer: D (LEAVE A REPLY)

NEW QUESTION: 45

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: 46

What is a difference from the list below between quantitative and qualitative Risk Assessment?

A. Qualitative risk assessments map to business objectives

B. Quantitative risk assessments result in an exact number (in monetary terms)

C. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

D. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Answer: (SHOW ANSWER)

NEW QUESTION: 47

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? (choose the best answer):
A. Configure your syslog to send SMS messages to current staff when target events are triggered
B. Deploy a SEIM solution and have current staff review incidents first thing in the morning
C. Employ an assumption of breach protocol and defend only essential information resources
D. Contract with a managed security provider and have current staff on recall for incident response
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
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.
The organization has already been subject to a significant amount of credit card fraud.
Which of the following is the MOST likely reason for this fraud?
A. Lack of compliance to the Payment Card Industry (PCI) standards
B. Security practices not in alignment with ISO 27000 frameworks
C. Lack of technical controls when dealing with credit card data
D. Ineffective security awareness program
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
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. Payment Card Industry Data Security Standards (PCI-DSS)
C. International Organization for Standardizations - 27005 (ISO-27005)
D. National Institute for Standards and Technology 800-50 (NIST 800-50)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following is a major benefit of applying risk levels?
A. Risk management governance becomes easier since most risks remain low once mitigated
B. Risk appetite can increase within the organization once the levels are understood

C. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology
D. Resources are not wasted on risks that are already managed to an acceptable level
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
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. Have a risk assessment performed.
B. Nothing, this falls outside your area of influence.
C. Close and chain the door shut and send a company-wide memo banning the practice.
D. Post a guard at the door to maintain physical security
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
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. A lack of executive presence within the security program
B. Poor audit support for the security program
C. This is normal since business units typically resist security requirements
D. Poor alignment of the security program to business needs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
The PRIMARY objective of security awareness is to:
A. Ensure that security policies are read.
B. Encourage security-conscious employee behavior.
C. Meet legal and regulatory requirements.
D. Put employees on notice in case follow-up action for noncompliance is necessary
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which of the following is the MAIN security concern for public cloud computing?
A. Unable to patch systems as needed
B. Unable to run anti-virus scans
C. Unable to track log on activity
D. Unable to control physical access to the servers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
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. Fully trained network forensic experts to analyze all data right after the attack
C. Expert forensics witness
D. Uninterrupted Chain of Custody
Answer: (SHOW ANSWER)

NEW QUESTION: 56
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: (SHOW ANSWER)

NEW QUESTION: 57
From an information security perspective, information that no longer supports the main purpose of the business should be:
A. protected under the information classification policy
B. analyzed under the data ownership policy
C. assessed by a business impact analysis.
D. analyzed under the retention policy.
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 58
When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?
A. Recovery
B. Eradication
C. Containment
D. Escalation
Answer: (SHOW ANSWER)

NEW QUESTION: 59

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 certifications, strong technical capabilities and lengthy resume
B. Multiple references, strong background check and industry certifications
C. Industry certifications, technical knowledge and program management skills
D. College degree, audit capabilities and complex project management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 60
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: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 61
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?
A. A substantive test of program library controls
B. A compliance test of the program compiler controls
C. A substantive test of the program compiler controls
D. A compliance test of program library controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62

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

NEW QUESTION: 63
While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?
A. Business continuity plan
B. Application mapping document
C. Disaster recovery strategic plan
D. Enterprise Risk Assessment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?
A. All vulnerabilities that impact important production servers
B. Only critical and high vulnerabilities that impact important production servers
C. All vulnerabilities found on servers and desktops
D. Only critical and high vulnerabilities on servers and desktops
Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?
A. Statement of Work
B. Service Level Agreements (SLA)
C. Terms and Conditions
D. Key Performance Indicators (KPI)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
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. Lack of version/source controls

B. Lack of change management controls
C. High turnover in the application development department
D. Ineffective configuration management controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
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: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following is considered the MOST effective tool against social engineering?
A. Effective Security Vulnerability Management Program
B. Effective Security awareness program
C. Anti-malware tools
D. Anti-phishing tools
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
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. Security Administrators
D. Risk Management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?
A. Plan-Select-Implement-Evaluate
B. Plan-Check-Do-Act
C. SCORE (Security Consensus Operational Readiness Evaluation)
D. Plan-Do-Check-Act

Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
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. Data breach disclosure
B. Consumer right disclosure
C. Special circumstance disclosure
D. Security incident disclosure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following backup sites takes the longest recovery time?
A. Mobile backup site
B. Warm site
C. Hot site
D. Cold site
Answer: (SHOW ANSWER)

NEW QUESTION: 73
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?
A. The organization uses exclusively a qualitative process to measure risk
B. The organization's risk tolerance is low
C. The organization uses exclusively a quantitative process to measure risk
D. The organization's risk tolerance is high
Answer: D (LEAVE A REPLY)

NEW QUESTION: 74
The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?
A. The remediation costs are irrelevant; it must be implemented regardless of cost.
B. The asset being protected is less valuable than the remediation costs
C. The audit finding is incorrect
D. The asset is more expensive than the remediation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
The ultimate goal of an IT security projects is:
A. Complete security

B. Implement information security policies
C. Support business requirements
D. Increase stock value
Answer: (SHOW ANSWER)

NEW QUESTION: 76
An example of professional unethical behavior is:
A. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
B. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation
C. Storing client lists and other sensitive corporate internal documents on a removable thumb drive
D. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
To make sure that the actions of all employees, applications, and systems follow the organization's rules and regulations can BEST be described as which of the following?
A. Risk management
B. Compliance management
C. Asset management
D. Security management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
A method to transfer risk is to:
A. Alignment with business operations
B. purchase breach insurance
C. Implement redundancy
D. move operations to another region

Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
When analyzing and forecasting a capital expense budget what are not included?
A. Upgrade of mainframe
B. Network connectivity costs
C. Purchase of new mobile devices to improve operations
D. New datacenter to operate from
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
What is the primary reason for performing vendor management?
A. To establish a vendor selection process
B. To understand the risk coverage that are being mitigated by the vendor
C. To define the partnership for long-term success
D. To document the relationship between the company and the vendor
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
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. Compliance centric agenda
B. IT security centric agenda
C. Lack of risk management process
D. Lack of risk management process
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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. Containment
C. Recovery
D. Identification
Answer: (SHOW ANSWER)

Explanation/Reference:

NEW QUESTION: 83
A security manager regularly checks work areas after business 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. Security awareness training
B. Audit validation
C. Physical control testing
D. Compliance management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
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. Review security procedures to determine if they need modified according to findings
B. Create detailed remediation funding and staffing plans
C. Validate the effectiveness of current controls
D. Report the audit findings and remediation status to business stake holders
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
Your organization provides open guest wireless access with no captive portals. What can you do to assist with law enforcement investigations if one of your guests is suspected of committing an illegal act using your network?
A. Configure logging on each access point
B. Install a firewall software on each wireless access point.
C. Provide IP and MAC address
D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
What is one key difference between Capital expenditures and Operating expenditures?
A. Operating expense cannot be written off while Capital expense can
B. Capital expenditures allow for the cost to be depreciated over time and Operating does not
C. Capital expenses cannot include salaries and Operating expenses can

D. Operating expenses can be depreciated over time and Capital expenses cannot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following is a primary method of applying consistent configurations to IT systems?
A. Audits
B. Administration
C. Templates
D. Patching
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
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 that the repository of stolen data is 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. Destroy the repository of stolen data
C. Consult with other executives to develop an action plan
D. Contact your local law enforcement agency
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?
A. Incident response plan
B. Damage control plan
C. Disaster recovery plan
D. Business Continuity plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
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 a Disaster Recovery (DR) exercise every year to test the plan
C. Outsource the creation and execution of the BC plan to a third party vendor
D. Conduct periodic tabletop exercises to refine the BC plan
Answer: (SHOW ANSWER)

NEW QUESTION: 91
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. Alignment with the business
C. Leveraging existing implementations
D. Proper budget management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the BEST control to safeguard data integrity?
A. Backup to a remote location
B. Maintain separate VM backups
C. Increase VM replication frequency
D. Backup to tape
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
What key technology can mitigate ransomware threats?
A. Phishing exercises
B. Blocking use of wireless networks
C. Application of multiple end point anti-malware solutions
D. Use immutable data storage

Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
An organization information security policy serves to
A. define security configurations for systems
B. define relationships with external law enforcement agencies
C. establish acceptable systems and user behavior
D. establish budgetary input in order to meet compliance requirements
Answer: C (LEAVE A REPLY)

NEW QUESTION: 95
The process of identifying and classifying assets is typically included in the
A. Business Impact Analysis
B. Disaster Recovery plan
C. Threat analysis process
D. Asset configuration management process
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following methodologies references the recommended industry standard that Information security project managers should follow?
A. Project Management Body of Knowledge
B. The Security Systems Development Life Cycle
C. Project Management System Methodology
D. The Security Project And Management Methodology
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?
A. Statements of Work
B. Key Performance Indicators (KPI)
C. Terms and Conditions
D. Service Level Agreements (SLA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 98
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: 99
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. Lack of reporting of a successful denial of service attack on the network.
C. Lack of notification to the public of disclosure of confidential information
D. Failure to notify police of an attempted intrusion
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following statements about Encapsulating Security Payload (ESP) is true?
A. It is an IPSec protocol.
B. It uses TCP port 22 as the default port and operates at the application layer.
C. It is a text-based communication protocol.
D. It uses UDP port 22
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
Acceptable levels of information security risk tolerance in an organization should be determined by?
A. Corporate legal counsel
B. CISO with reference to the company goals
C. CEO and board of director
D. Corporate compliance committee
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
Risk appetite is typically determined by which of the following organizational functions?
A. Business units
B. Security
C. Board of Directors
D. Audit and compliance
Answer: (SHOW ANSWER)

NEW QUESTION: 103

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: 104
Which of the following is true regarding expenditures?
A. Capital expenditures are never taxable
B. Operating expenditures are for acquiring assets, capital expenditures are for support costs of that asset
C. Capital expenditures are used to define depreciation tables of intangible assets
D. Capital expenditures are for acquiring assets, whereas operating expenditures are for support costs of that
Answer: (SHOW ANSWER)
asset

NEW QUESTION: 105
When creating contractual agreements and procurement processes why should security requirements be included?
A. To make sure the security process aligns with the vendor's security process
B. To make sure the costs of security is included and understood
C. To make sure they are added on after the process is completed
D. To make sure the patching process is included with the costs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
Why is it vitally important that senior management endorse a security policy?
A. So that they will accept ownership for security within the organization.
B. So that they can be held legally accountable.
C. So that employees will follow the policy directives.
D. So that external bodies will recognize the organizations commitment to security.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
Which business stakeholder is accountable for the integrity of a new information system?
A. Compliance Officer
B. CISO
C. Project manager
D. Board of directors
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 108
The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?
A. Establishing Enterprise-owned Botnets for preemptive attacks
B. Collaboration with law enforcement
C. Be able to retaliate under the framework of Active Defense
D. Well established and defined digital forensics process
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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.
The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization.
From an organizational perspective, which of the following is the LIKELY reason for this?
A. The CISO has not implemented a security awareness program
B. The CISO has not implemented a policy management framework
C. The CISO reports to the IT organization
D. The CISO does not report directly to the CEO of the organization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
The new CISO was informed of all the Information Security projects that the organization has in progress. Two projects are over a year behind schedule and over budget. Using

best business practices for project management you determine that the project correctly aligns with the company goals.
Which of the following needs to be performed NEXT?
A. Verify the scope of the project
B. Verify the regulatory requirements
C. Verify technical resources
D. Verify capacity constraints
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN.
What type of control is being implemented by supervisors and data owners?
A. Operational
B. Management
C. Administrative
D. Technical
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
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 would be the FIRST step when addressing Information Security formally and consistently in this organization?
A. Define formal roles and responsibilities for Information Security
B. Define formal roles and responsibilities for Internal audit functions
C. Create an executive security steering committee
D. Contract a third party to perform a security risk assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

A. Upper management support
B. More frequent project milestone meetings
C. More training of staff members
D. Involve internal audit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114
What is the main purpose of the Incident Response Team?
A. Communicate details of information security incidents
B. Create effective policies detailing program activities
C. Provide current employee awareness programs
D. Ensure efficient recovery and reinstate repaired systems
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
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. The organization has already been subject to a significant amount of credit card fraud.
Which of the following is the MOST likely reason for this fraud?
A. Lack of compliance to the Payment Card Industry (PCI) standards
B. Ineffective security awareness program
C. Lack of technical controls when dealing with credit card data
D. Security practices not in alignment with ISO 27000 frameworks
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 116
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 asset owner
B. The project manager
C. The asset manager
D. The data custodian
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
Which business stakeholder is accountable for the integrity of a new information system?
A. CISO
B. Compliance Officer

C. Project manager
D. Board of directors
Answer: A (LEAVE A REPLY)
ECCouncil 712-50 : Practice Test

NEW QUESTION: 118
What is the FIRST step in developing the vulnerability management program?
A. Organization Vulnerability
B. Define Policy
C. Maintain and Monitor
D. Baseline the Environment
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Credit card information, medical data, and government records are all examples of:
A. Confidential/Protected Information
B. Bodily Information
C. Communications Information
D. Territorial Information
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?
A. Meet legal requirements
B. Better understand the threats and vulnerabilities affecting the environment
C. Better understand strengths and weaknesses of the program
D. Meet regulatory compliance requirements
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?
A. Determine the risk tolerance
B. Perform an asset classification
C. Create an architecture gap analysis
D. Analyze existing controls on systems
Answer: B (LEAVE A REPLY)

NEW QUESTION: 122
While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?
A. Application mapping document
B. Business continuity plan
C. Disaster recovery strategic plan
D. Enterprise Risk Assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 123
In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?
A. Vmware, router, switch, firewall, syslog, vulnerability management system (VMS)
B. SIEM, IDS, firewall, VMS
C. Security Incident Event Management (SIEM), IDS, router, syslog
D. Intrusion Detection System (IDS), firewall, switch, syslog
Answer: (SHOW ANSWER)

NEW QUESTION: 124
You have implemented the new controls. What is the next step?
A. Perform a risk assessment
B. Document the process for the stakeholders
C. Update the audit findings report
D. Monitor the effectiveness of the controls
Answer: (SHOW ANSWER)

NEW QUESTION: 125
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 is unsure of the information provided and orders a vendor proof of concept to validate the system's scalability.
This demonstrates which of the following?
A. A risk-based approach to determine if the solution is suitable for investment
B. A methodology-based approach to ensure authentication mechanism functions
C. An approach that allows for minimum budget impact if the solution is unsuitable
D. An approach providing minimum time impact to the implementation schedules
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient.
Which of the following keys should be used to encrypt the message?
A. the recipient's private key
B. Certificate authority key
C. The recipient's public key
D. Your public key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 127
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?
A. Conduct periodic tabletop exercises to refine the BC plan
B. Test every three years to ensure that things work as planned
C. Outsource the creation and execution of the BC plan to a third party vendor
D. Conduct a Disaster Recovery (DR) exercise every year to test the plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
Who is responsible for verifying that audit directives are implemented?
A. Internal Audit
B. IT Security
C. BOD Audit Committee
D. IT Management
Answer: (SHOW ANSWER)

NEW QUESTION: 129
A method to transfer risk is to_____.
A. Implement redundancy
B. Move operations to another region
C. Alignment with business operations

D. Purchase breach insurance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
Risk that remains after risk mitigation is known as_____.
A. Residual risk
B. Persistent risk
C. Non-tolerated risk
D. Accepted risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 131
Creating a secondary authentication process for network access would be an example of?
A. Putting undue time commitment on the system administrator.
B. Supporting the concept of layered security
C. An administrator with too much time on their hands.
D. Network segmentation.
Answer: (SHOW ANSWER)

NEW QUESTION: 132
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 audit support for the security program
B. Poor alignment of the security program to business needs
C. This is normal since business units typically resist security requirements
D. A lack of executive presence within the security program
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 133
The ultimate goal of an IT security projects is:
A. Support business requirements
B. Increase stock value
C. Implement information security policies
D. Complete security
Answer: A (LEAVE A REPLY)

NEW QUESTION: 134
When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

A. How many servers do you have?
B. What is the value of the assets at risk?
C. How many credit card records are stored?
D. What is the scope of the certification?
Answer: (SHOW ANSWER)