EC-COUNCIL.712-50.v2023-01-10.q114

Exam Code:	712-50
Exam Name:	EC-Council Certified CISO (CCISO)
Certification Provider:	EC-COUNCIL
Free Question Number:	114
Version:	v2023-01-10
# of views:	1367
# of Questions views:	1140
https://www.freeqas.com/qa/EC-COUNCIL/712-50/EC-COUNCIL.712-50.v2023-01-10.q114.html	

NEW QUESTION: 1
Which of the following represents the BEST method of ensuring security program alignment to business needs?
A. Ensure security implementations include business unit testing and functional validation prior to production rollout
B. Create a comprehensive security awareness program and provide success metrics to business units
C. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role
D. Create security consortiums, such as strategic security planning groups, that include business unit participation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following provides an audit framework?
A. National Institute of Standards and Technology (NIST) SP 800-30
B. International Organization Standard (ISO) 27002
C. Control Objectives for IT (COBIT)
D. Payment Card Industry-Data Security Standard (PCI-DSS)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
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. Cite compliance with laws, statutes, and regulations - explaining the financial implications for the company for non-compliance
C. Draw from your experience and recount stories of how other companies have been compromised
D. Understand the business and focus your efforts on enabling operations securely
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
An organization information security policy serves to_____.
A. define relationships with external law enforcement agencies
B. establish acceptable systems and user behavior
C. None
D. define security configurations for systems
E. establish budgetary input in order to meet compliance requirements
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do.
What can John do in this instance?
A. refer to the contract agreement for direction.
B. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
C. Review the Request for proposal (RFP) for guidance.
D. Withhold the vendor's payments until the issue is resolved.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
Dataflow diagrams are used by IT auditors to:
A. Graphically summarize data paths and storage processes.
B. Highlight high-level data definitions.
C. Order data hierarchically.
D. Portray step-by-step details of data generation.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?
A. Dual Control
B. Separation of Duties
C. Least Privilege
D. Split Knowledge
Answer: A (LEAVE A REPLY)

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- factor implementation project?
A. Decide to accept the risk on behalf of the impacted business units
B. Create new use cases for operational use of the solution
C. Report the deficiency to the audit team and create process exceptions
D. Determine if sufficient mitigating controls can be applied
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 9
As the CISO you need to write the IT security strategic plan.
Which of the following is the MOST important to review before you start writing the plan?
A. The present IT budget
B. The company business plan
C. Other corporate technology trends
D. The existing IT environment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
When briefing senior management on the creation of a governance process, the MOST important aspect should be:
A. knowledge required to analyze each issue.
B. information security metrics.

C. baseline against which metrics are evaluated.
D. linkage to business area objectives.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
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 periodic examination of access rights
B. Lack of reporting of a successful denial of service attack on the network.
C. Failure to notify police of an attempted intrusion
D. Lack of notification to the public of disclosure of confidential information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
The formal certification and accreditation process has four primary steps, what are they?
A. Evaluating, describing, testing and authorizing
B. Auditing, documenting, verifying, certifying
C. Evaluating, purchasing, testing, authorizing
D. Discovery, testing, authorizing, certifying
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 13
The PRIMARY objective of security awareness is to:
A. Put employees on notice in case follow-up action for noncompliance is necessary
B. Meet legal and regulatory requirements.
C. Ensure that security policies are read.
D. Encourage security-conscious employee behavior.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
You have implemented the new controls. What is the next step?
A. Document the process for the stakeholders
B. Update the audit findings report
C. Perform a risk assessment
D. Monitor the effectiveness of the controls
Answer: (SHOW ANSWER)

NEW QUESTION: 15

The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:
A. Single Loss Expectancy
B. Life Cycle Loss Expectancy
C. Safeguard Value
D. Cost Benefit Analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.
Using the best business practices for project management you determine that the project correct aligns with the company goals. What needs to be verified FIRST?
A. Vendor for the project
B. Scope of the project
C. Timeline of the project milestones
D. Training of the personnel on the project
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?
A. Business Continuity plan
B. Disaster recovery plan
C. Damage control plan
D. Incident response plan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
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: 19
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: D (LEAVE A REPLY)

NEW QUESTION: 20
From an information security perspective, information that no longer supports the main purpose of the business should be:
A. assessed by a business impact analysis.
B. protected under the information classification policy
C. analyzed under the data ownership policy
D. analyzed under the retention policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
When selecting a security solution with reoccurring maintenance costs after the first year
A. Implement the solution and ask for the increased operating cost budget when it is time
B. Defer selection until the market improves and cash flow is positive
C. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
D. The CISO should cut other essential programs to ensure the new solution's continued use
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22

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

NEW QUESTION: 23
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: A (LEAVE A REPLY)

NEW QUESTION: 24
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. Provide the business units with control mandates and schedules of audits for compliance validation
C. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
D. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
The ability to demand the implementation and management of security controls on third parties providing services to an organization is
A. Compliance management
B. Security Governance
C. Vendor management
D. Disaster recovery
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
An example of professional unethical behavior is:

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

NEW QUESTION: 27
During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:
A. Identify and evaluate existing controls.
B. Disclose the threats and impacts to management.
C. Identify and assess the risk assessment process used by management.
D. Identify information assets and the underlying systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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.
How can you reduce the administrative burden of distributing symmetric keys for your employer?
A. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it
B. Use asymmetric encryption for the automated distribution of the symmetric key
C. Use a self-generated key on both ends to eliminate the need for distribution
D. Use certificate authority to distribute private keys
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
The Board of Directors of a publicly-traded company is concerned about the security implications of a strategic project that will migrate 50% of the organization's information technology assets to the cloud. They have requested a briefing on the project plan and a progress report of the security stream of the project. As the CISO, you have been tasked with preparing the report for the Chief Executive Officer to present.
Using the Earned Value Management (EVM), what does a Cost Variance (CV) of -1,200 mean?
A. The project is under budget
B. The project budget has reserves

C. The project is over budget
D. The project cost is in alignment with the budget
Answer: (SHOW ANSWER)

NEW QUESTION: 30
You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?
A. Determine program ownership to implement compensating controls
B. Validate that security awareness program content includes information about the potential vulnerability
C. Conduct a thorough risk assessment against the current implementation to determine system functions
D. Send a report to executive peers and business unit owners detailing your suspicions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
When creating contractual agreements and procurement processes why should security requirements be included?
A. To make sure they are added on after the process is completed
B. To make sure the costs of security is included and understood
C. To make sure the security process aligns with the vendor's security process
D. To make sure the patching process is included with the costs
Answer: B (LEAVE A REPLY)
Scenario1

NEW QUESTION: 32
If your organization operates under a model of "assumption of breach", you should:
A. Protect all information resource assets equally
B. Establish active firewall monitoring protocols
C. Focus your security efforts on high value assets
D. Purchase insurance for your compliance liability

Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?
A. Risk Management
B. Risk Assessment
C. System Testing
D. Vulnerability Assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
When analyzing and forecasting an operating expense budget what are not included?
A. Utilities and power costs
B. Software and hardware license fees
C. Network connectivity costs
D. New datacenter to operate from
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
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. Strategic Risk
B. Compliance Risk
C. Reputation Risk
D. Operational Risk
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
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 qualitative risk assessment
B. Conduct a hybrid risk assessment
C. Conduct a subjective risk assessment
D. Conduct a quantitative risk assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?
A. Internal Firewall ruleset reviews
B. Perform a vulnerability scan of the network
C. External penetration testing by a qualified third party
D. Implement network intrusion prevention systems
Answer: (SHOW ANSWER)

NEW QUESTION: 38
The success of the Chief Information Security Officer is MOST dependent upon:
A. favorable audit findings
B. following the recommendations of consultants and contractors
C. development of relationships with organization executives
D. raising awareness of security issues with end users
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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 change management controls
B. High turnover in the application development department
C. Ineffective configuration management controls
D. Lack of version/source controls
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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. Software removal, install software patch, maintain system
C. Install software patch, Operate system, Maintain system
D. Discover software, Remove affected software, Apply software patch
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
File Integrity Monitoring (FIM) is considered a
A. User segmentation control

B. Security detective control
C. Software segmentation control
D. Network based security preventative control
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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. Semi-annually
B. Bi-annually
C. Quarterly
D. Annually
Answer: D (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. Forensic experts
B. External Audit
C. Penetration testers
D. Internal Audit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following is considered one of the most frequent failures in project management?
A. Insufficient resources
B. Overly restrictive management
C. Excessive personnel on project
D. Failure to meet project deadlines
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following is considered one of the most frequent failures in project management?
A. Overly restrictive management
B. Insufficient resources
C. Excessive personnel on project
D. Failure to meet project deadlines
Answer: D (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 46
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 a formal security policy governance process
D. Lack of formal definition of roles and responsibilities
Answer: (SHOW ANSWER)

NEW QUESTION: 47
The ultimate goal of an IT security projects is:
A. Support business requirements
B. Complete security
C. Increase stock value
D. Implement information security policies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
Which technology can provide a computing environment without requiring a dedicated hardware backend?
A. Virtual Desktop
B. Virtual Local Area Network
C. Mainframe server
D. Thin client
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49

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 proper access controls
B. Lack of asset management processes
C. lack of change management processes
D. Lack of hardening standards
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
What is the MOST critical output of the incident response process?
A. A complete document of all involved team members and the support they provided
B. Clearly defined documents detailing standard evidence collection and preservation processes
C. Lessons learned from the incident, so they can be incorporated into the incident response processes
D. Recovery of all data from affected systems
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
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: 52
The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?
A. Explain to the IT group that the IPS won't cause any network impact because it will fail open
B. Work with the IT group and tell them to put IPS in-line and say it won't cause any network impact
C. Explain to the IT group that the IPS will fail open once in-line however it will be deployed in monitor mode for a set period of time to ensure that it doesn't block any legitimate traffic

D. Explain to the IT group that this is a business need and the IPS will fail open however, if there is a network failure the CISO will accept responsibility
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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 Care
C. Due Protection
D. Due process
Answer: (SHOW ANSWER)

NEW QUESTION: 54
The total cost of security controls should:
A. be less than the value of the information resource being protected
B. Be greater than the value of the information resource being protected
C. Should not matter, as long as the information resource is protected
D. Be equal to the value information resource being protected
Answer: (SHOW ANSWER)

NEW QUESTION: 55
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: 56
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." Which group of people should be consulted when developing your security program?
A. All of the above
B. End Users
C. Peers
D. Executive Management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
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. At the time the security services are being performed and the vendor needs access to the network
B. Prior to signing the agreement and before any security services are being performed
C. Once the vendor is on premise and before they perform security services
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: 58
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. Data Loss Prevention (DLP)
B. Rigorous syslog reviews
C. Security Guards posted outside the Data Center
D. Intrusion Detection Systems (IDS)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
Which of the following defines the boundaries and scope of a risk assessment?
A. The risk assessment framework
B. The risk assessment charter
C. The assessment context
D. The risk assessment schedule
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
The rate of change in technology increases the importance of:
A. Implementing and enforcing good processes.
B. Outsourcing the IT functions.
C. Hiring personnel with leading edge skills.
D. Understanding user requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
The main purpose of the SOC is:
A. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation
B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities
C. An organization which provides Tier 1 support for technology issues and provides escalation when needed
D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
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 normal definition of roles and responsibilities
B. Lack of a formal security awareness program
C. Lack of a formal security policy governance process
D. Lack of a formal risk management policy
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What key technology can mitigate ransomware threats?
A. Use immutable data storage
B. Phishing exercises
C. Blocking use of wireless networks
D. Application of multiple end point anti-malware solutions
Answer: (SHOW ANSWER)

NEW QUESTION: 64
The success of the Chief Information Security Officer is MOST dependent upon:
A. raising awareness of security issues with end users
B. development of relationships with organization executives
C. favorable audit findings
D. following the recommendations of consultants and contractors
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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: 66
When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?
A. Weekly
B. Daily
C. Hourly
D. Monthly
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
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. Post a guard at the door to maintain physical security
B. Close and chain the door shut and send a company-wide memo banning the practice
C. Have a risk assessment performed
D. Nothing, this falls outside your area of influence
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 68
Which of the following is the BEST indicator of a successful project?
A. it is completed on time or early as compared to the baseline project plan
B. it meets most of the specifications as outlined in the approved project definition
C. the deliverables are accepted by the key stakeholders
D. it comes in at or below the expenditures planned for in the baseline budget
Answer: (SHOW ANSWER)

NEW QUESTION: 69
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?
A. Outsource the creation and execution of the BC plan to a third party vendor
B. Conduct periodic tabletop exercises to refine the BC plan
C. Conduct a Disaster Recovery (DR) exercise every year to test the plan
D. Test every three years to ensure that things work as planned
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
The patching and monitoring of systems on a consistent schedule is required by?
A. Audit best practices
B. Risk Management framework
C. Local privacy laws
D. Industry best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Which of the following statements below regarding Key Performance indicators (KPIs) are true?
A. They are a strictly qualitative measure of success
B. They should be standard throughout the organization versus domain-specific so they are more easily correlated
C. They are a strictly quantitative measure of success
D. Development of KPI's are most useful when done independently

Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
A method to transfer risk is to:
A. purchase breach insurance
B. Implement redundancy
C. move operations to another region
D. Alignment with business operations
Answer: (SHOW ANSWER)

NEW QUESTION: 73
What type of attack requires the least amount of technical equipment and has the highest success rate?
A. Operating system attacks
B. Shrink wrap attack
C. Social engineering
D. War driving
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
An organization has implemented a change management process for all changes to the IT production environment. This change management process follows best practices and is expected to help stabilize the availability and integrity of the organization's IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process?
A. Number of change orders processed
B. Number of change orders rejected
C. Number and length of planned outages
D. Number of unplanned outages
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The cipher text sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?
A. None
B. Asynchronous
C. Open
D. Shared key
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
One of the MAIN goals of a Business Continuity Plan is to_____.
A. Ensure all infrastructure and applications are available in the event of a disaster
B. Assign responsibilities to the technical teams responsible for the recovery of all data
C. Allow all technical first-responders to understand their roles in the event of a disaster.
D. Provide step by step plans to recover business processes in the event of a disaster
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process.
Which of the following represents your BEST course of action?
A. Conduct a throughout risk assessment against the current implementation to determine system functions
B. Send a report to executive peers and business unit owners detailing your suspicions
C. Validate that security awareness program content includes information about the potential vulnerability
D. Determine program ownership to implement compensating controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
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. Contract a third party to perform a security risk assessment
B. Define formal roles and responsibilities for Information Security
C. Define formal roles and responsibilities for Internal audit functions
D. create an executive security steering committee
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
A stakeholder is a person or group:
A. That has budget authority.
B. Vested in the success and/or failure of a project or initiative regardless of budget implications.
C. That will ultimately use the system.
D. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
The ability to demand the implementation and management of security controls on third parties providing services to an organization is
A. Security Governance
B. Vendor management
C. Compliance management
D. Disaster recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 81
When selecting a security solution with reoccurring maintenance costs after the first year, the CISO should: (choose the BEST answer)
A. Defer selection until the market improves and cash flow is positive
B. Communicate future operating costs to the CIO/CFO and seek commitment from them 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. The CISO should cut other essential programs to ensure the new solution's continued use
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
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 an auditing methodology in place.
C. There is a clear definition of the IT security mission and vision.
D. The plan requires return on investment for all security projects.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83

The general ledger setup function in an enterprise resource package allows for setting accounting periods. Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

A. The lack of policies and procedures for the proper segregation of duties.

B. The need to create and modify the chart of accounts and its allocations.

C. The need to change accounting periods on a regular basis.

D. The requirement to post entries for a closed accounting period.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 84

As the CISO you need to write the IT security strategic plan. Which of the following is the MOST important to review before you start writing the plan?

A. The existing IT environment.

B. The company business plan.

C. Other corporate technology trends.

D. The present IT budget.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 85

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. Perform an asset classification

B. Determine the risk tolerance

C. Analyze existing controls on systems

D. Create an architecture gap analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 86

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. Third-party emergency repair contract

B. Pre-built servers and routers

C. Permanent alternative routing

D. Full off-site backup of every server

Answer: C (LEAVE A REPLY)

NEW QUESTION: 87

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 security awareness program
C. The CISO has not implemented a policy management framework
D. The CISO does not report directly to the CEO of the organization
Answer: A (LEAVE A REPLY)

NEW QUESTION: 88
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: 89
The alerting, monitoring and life-cycle management of security related events is typically handled by the_____.
A. security threat and vulnerability management process
B. risk assessment process
C. risk management process
D. governance, risk, and compliance tools
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Dataflow diagrams are used by IT auditors to:
A. Graphically summarize data paths and storage processes.
B. Order data hierarchically
C. Highlight high-level data definitions
D. Portray step-by-step details of data generation.
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 91

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?
A. Threat
B. Attack vector
C. Vulnerability
D. Exploitation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
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.
Recently, members of your organization have been targeted through a number of sophisticated phishing attempts and have compromised their system credentials. What action can you take to prevent the misuse of compromised credentials to change bank account information from outside your organization while still allowing employees to manage their bank information?
A. Turn off VPN access for users originating from outside the country
B. Force a change of all passwords
C. Enable monitoring on the VPN for suspicious activity
D. Block access to the Employee-Self Service application via VPN
Answer: D (LEAVE A REPLY)

NEW QUESTION: 93
At what level of governance are individual projects monitored and managed?
A. Program
B. Milestone

C. Enterprise
D. Portfolio
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
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. Security roadmap
B. Business Continuity plan
C. Annual report to shareholders
D. Business Impact Analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
What is a Statement of Objectives (SOA)?
A. A document that outlines specific desired outcomes as part of a request for proposal
B. A section of a contract that defines tasks to be performed under said contract
C. Business guidance provided by the CEO
D. An outline of what the military will do during war
Answer: (SHOW ANSWER)

NEW QUESTION: 96
What oversight should the information security team have in the change management process for application security?
A. Development team should tell the information security team about any application security flaws
B. Information security should be aware of all application changes and work with developers before changes are deployed in production
C. 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
D. Information security should be informed of changes to applications only
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
Human resource planning for security professionals in your organization is a:
A. Simple and easy task because the threats are getting easier to find and correct.
B. Training requirement that is on-going and always changing.

C. Training requirement that is met through once every year user training.
D. Not needed because automation and anti-virus software has eliminated the threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
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: 99
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. Ensure all infrastructure and applications are available in the event of a disaster
C. Allow all technical first-responders to understand their roles in the event of a disaster
D. Provide step by step plans to recover business processes in the event of a disaster
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following is a major benefit of applying risk levels?
A. Risk appetite increase within the organization once the levels are understood
B. Risk management governance becomes easier since most risks remain low once mitigated
C. Resources are not wasted on risks that are already managed to an acceptable level
D. Risk budgets are more easily managed due to fewer due to fewer identified risks as a result of using a methodology
Answer: C (LEAVE A REPLY)

NEW QUESTION: 101
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 agreement has been signed and the security vendor states that they will need access to the network
B. At the time the security services are being performed and the vendor needs access to the network
C. Once the vendor is on premise and before they perform security services

D. Prior to signing the agreement and before any security services are being performed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?
A. Implementation of it eases an organization's auditing and compliance burden
B. Information Security (IS) procedures often require augmentation with other standards
C. It allows executives to more effectively monitor IT implementation costs
D. It provides for a consistent and repeatable staffing model for technology organizations
Answer: (SHOW ANSWER)

NEW QUESTION: 103
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.
When formulating the remediation plan, what is a required input?
A. Board of directors
B. Risk assessment
C. Patching history
D. Latest virus definitions file
Answer: (SHOW ANSWER)
Scenario6

NEW QUESTION: 104
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: 105
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the

Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.
Your Corporate Information Security Policy should include which of the following?
A. Information security theory
B. Incident response contacts
C. Desktop configuration standards
D. Roles and responsibilities
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
Which of the following is a symmetric encryption algorithm?
A. MD5
B. RSA
C. 3DES
D. ECC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO).
The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?
A. ISO 22301 BCM Requirements
B. ISO 27031 BCM Readiness
C. ISO 22318 Supply Chain Continuity
D. ISO 22317 BIA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
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: 109
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-line and turn on blocking mode to stop malicious traffic.
C. In promiscuous mode and block malicious traffic.
D. In promiscuous mode and only detect malicious traffic.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
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?
A. Rigorous syslog reviews
B. Data Loss Prevention (DLP)
C. Security Guards posted outside the Data Center
D. Intrusion Detection Systems (IDS)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
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: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 112
The organization does not have the time to remediate the vulnerability; however it is critical to release the application. Which of the following needs to be further evaluated to help mitigate the risks?
A. Provide developer security training
B. Provide security testing tools
C. Implement Compensating Controls
D. Deploy Intrusion Detection Systems
Answer: (SHOW ANSWER)

NEW QUESTION: 113
The process of creating a system which divides documents based on their security level to manage access to private data is known as _____.
A. Privacy protection
B. security coding
C. data classification
D. data security system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?
A. Human Resources and Budget
B. Budget and Compliance
C. Legal and Human Resources
D. Audit and Legal
Answer: D (LEAVE A REPLY)