Exam Questions 712-50

EC-Council Certified CISO (CCISO)

https://www.2passeasy.com/dumps/712-50/

NEW QUESTION 1
- (Exam Topic 6)
An auditor is reviewing the security classifications for a group of assets and finds that many of the assets are not correctly classified.
What should the auditor's NEXT step be?

A. Immediately notify the board of directors of the organization as to the finding
B. Correct the classifications immediately based on the auditor's knowledge of the proper classification
C. Document the missing classifications
D. Identify the owner of the asset and induce the owner to apply a proper classification

Answer: C

NEW QUESTION 2
- (Exam Topic 6)
What is the primary difference between regulations and standards?

A. Standards will include regulations
B. Standards that aren't followed are punishable by fines
C. Regulations are made enforceable by the power provided by laws
D. Regulations must be reviewed and approved by the business

Answer: C

NEW QUESTION 3
- (Exam Topic 6)
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. Recovery of all data from affected systems
C. Lessons learned from the incident, so they can be incorporated into the incident response processes
D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: C

Explanation:
Reference: https://www.eccouncil.org/incident-response-plan-phases/

NEW QUESTION 4
- (Exam Topic 6)
A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

A. Public cloud
B. Private cloud
C. Community cloud
D. Hybrid cloud

Answer: D

Explanation:
Reference:
https://www.datacenters.com/services/cloud-services#:~:text=Hybrid%20clouds%20combine%20public%20and

NEW QUESTION 5
- (Exam Topic 6)
Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person's eye.
However, authorization failures can occur with individuals who have?

A. Glaucoma or cataracts
B. Two different colored eyes (heterochromia iridium)
C. Contact lens
D. Malaria

Answer: A

NEW QUESTION 6
- (Exam Topic 6)
Which of the following strategies provides the BEST response to a ransomware attack?

A. Real-time off-site replication
B. Daily incremental backup
C. Daily full backup
D. Daily differential backup

Answer: B

NEW QUESTION 7
- (Exam Topic 6)
What does RACI stand for?

A. Reasonable, Actionable, Controlled, and Implemented
B. Responsible, Actors, Consult, and Instigate
C. Responsible, Accountable, Consulted, and Informed
D. Review, Act, Communicate, and Inform

Answer: C

Explanation:
Reference: https://www.google.com/search?q=What+does+RACI+stand+for&oq=What+does+RACI+stand+for&aqs=edge

NEW QUESTION 8
- (Exam Topic 6)
An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.
What is the MOST likely reason why the sensitive data was posted?

A. The DLP Solution was not integrated with mobile device anti-malware
B. Data classification was not properly performed on the assets
C. The sensitive data was not encrypted while at rest
D. A risk assessment was not performed after purchasing the DLP solution

Answer: D

NEW QUESTION 9
- (Exam Topic 6)
What is a Statement of Objectives (SOA)?

A. A section of a contract that defines tasks to be performed under said contract
B. An outline of what the military will do during war
C. A document that outlines specific desired outcomes as part of a request for proposal
D. Business guidance provided by the CEO

Answer: A

NEW QUESTION 10
- (Exam Topic 6)
Who is responsible for verifying that audit directives are implemented?

A. IT Management
B. Internal Audit
C. IT Security
D. BOD Audit Committee

Answer: B

Explanation:
Reference: https://www.eccouncil.org/information-security-management/

NEW QUESTION 10
- (Exam Topic 6)
A Security Operations (SecOps) Manager is considering implementing threat hunting to be able to make better decisions on protecting information and assets.
What is the MAIN goal of threat hunting to the SecOps Manager?

A. Improve discovery of valid detected events
B. Enhance tuning of automated tools to detect and prevent attacks
C. Replace existing threat detection strategies
D. Validate patterns of behavior related to an attack

Answer: A

Explanation:
Reference:
https://www.techtarget.com/searchsecurity/feature/7-SecOps-roles-and-responsibilities-for-the-modern-enterpris

NEW QUESTION 15
- (Exam Topic 2)
Which of the following is a benefit of a risk-based approach to audit planning?

A. Resources are allocated to the areas of the highest concern
B. Scheduling may be performed months in advance
C. Budgets are more likely to be met by the IT audit staff
D. Staff will be exposed to a variety of technologies

Answer: A

NEW QUESTION 18
- (Exam Topic 2)
A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
D. If the findings do not impact regulatory compliance, review current security controls.

Answer: C

NEW QUESTION 19
- (Exam Topic 2)
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 program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls

Answer: B

NEW QUESTION 20
- (Exam Topic 2)
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. It allows executives to more effectively monitor IT implementation costs
B. Implementation of it eases an organization's auditing and compliance burden
C. Information Security (IS) procedures often require augmentation with other standards
D. It provides for a consistent and repeatable staffing model for technology organizations

Answer: B

NEW QUESTION 23
- (Exam Topic 1)
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

A. Test every three years to ensure that things work as planned
B. Conduct periodic tabletop exercises to refine the BC plan
C. Outsource the creation and execution of the BC plan to a third party vendor
D. Conduct a Disaster Recovery (DR) exercise every year to test the plan

Answer: B

NEW QUESTION 25
- (Exam Topic 1)
Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

A. Strong authentication technologies
B. Financial reporting regulations
C. Credit card compliance and regulations
D. Local privacy laws

Answer: D

NEW QUESTION 27
- (Exam Topic 1)
Which of the following is the MOST important benefit of an effective security governance process?

A. Reduction of liability and overall risk to the organization
B. Better vendor management
C. Reduction of security breaches
D. Senior management participation in the incident response process

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
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. Allow all technical first-responders to understand their roles in the event of a disaster
C. Provide step by step plans to recover business processes in the event of a disaster
D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer: C

NEW QUESTION 31
- (Exam Topic 1)
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. Vulnerability
C. Attack vector
D. Exploitation

Answer: B

NEW QUESTION 32
- (Exam Topic 1)
The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for

A. Confidentiality, Integrity and Availability
B. Assurance, Compliance and Availability
C. International Compliance
D. Integrity and Availability

Answer: A

NEW QUESTION 34
- (Exam Topic 1)
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

A. Reduction of budget
B. Decreased security awareness
C. Improper use of information resources
D. Fines for regulatory non-compliance

Answer: D

NEW QUESTION 36
- (Exam Topic 1)
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. Industry certifications, technical knowledge and program management skills
C. College degree, audit capabilities and complex project management
D. Multiple references, strong background check and industry certifications

Answer: B

NEW QUESTION 38
- (Exam Topic 1)
Which of the following is MOST important when dealing with an Information Security Steering committee:

A. Include a mix of members from different departments and staff levels.
B. Ensure that security policies and procedures have been vetted and approved.
C. Review all past audit and compliance reports.
D. Be briefed about new trends and products at each meeting by a vendor.

Answer: C

NEW QUESTION 40
- (Exam Topic 1)
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: A

NEW QUESTION 41

- (Exam Topic 1)
Who is responsible for securing networks during a security incident?

A. Chief Information Security Officer (CISO)
B. Security Operations Center (SO
C. Disaster Recovery (DR) manager
D. Incident Response Team (IRT)

Answer: D

NEW QUESTION 44
- (Exam Topic 1)
Which of the following intellectual Property components is focused on maintaining brand recognition?

A. Trademark
B. Patent
C. Research Logs
D. Copyright

Answer: A

NEW QUESTION 45
- (Exam Topic 1)
A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

A. Compliance to the Payment Card Industry (PCI) regulations.
B. Alignment with financial reporting regulations for each country where they operate.
C. Alignment with International Organization for Standardization (ISO) standards.
D. Compliance with patient data protection regulations for each country where they operate.

Answer: D

NEW QUESTION 50
- (Exam Topic 1)
Which of the following is considered the MOST effective tool against social engineering?

A. Anti-phishing tools
B. Anti-malware tools
C. Effective Security Vulnerability Management Program
D. Effective Security awareness program

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
A global retail company is creating a new compliance management process. Which of the following regulations is of MOST importance to be tracked and managed by this process?

A. Information Technology Infrastructure Library (ITIL)
B. International Organization for Standardization (ISO) standards
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. National Institute for Standards and Technology (NIST) standard

Answer: C

NEW QUESTION 58
- (Exam Topic 1)
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

A. They are objective and can express risk / cost in real numbers
B. They are subjective and can be completed more quickly
C. They are objective and express risk / cost in approximates
D. They are subjective and can express risk /cost in real numbers

Answer: A

NEW QUESTION 63
- (Exam Topic 1)
Which of the following should be determined while defining risk management strategies?

A. Organizational objectives and risk tolerance
B. Risk assessment criteria
C. IT architecture complexity
D. Enterprise disaster recovery plans

Answer: A

NEW QUESTION 64
- (Exam Topic 1)
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

A. National Institute for Standards and Technology 800-50 (NIST 800-50)
B. International Organization for Standardizations – 27005 (ISO-27005)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27004 (ISO-27004)

Answer: B

NEW QUESTION 69
- (Exam Topic 6)
You have been promoted to the CISO of a big-box retail store chain reporting to the Chief Information Officer (CIO). The CIO's first mandate to you is to develop a cybersecurity compliance framework that will meet all the store's compliance requirements.
Which of the following compliance standard is the MOST important to the organization?

A. The Federal Risk and Authorization Management Program (FedRAMP)
B. ISO 27002
C. NIST Cybersecurity Framework
D. Payment Card Industry (PCI) Data Security Standard (DSS)

Answer: D

Explanation:
Reference:
https://searchcompliance.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

NEW QUESTION 74
- (Exam Topic 6)
You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans.
Which control is MOST important to protect AI products?

A. Hash datasets
B. Sanitize datasets
C. Delete datasets
D. Encrypt datasets

Answer: D

NEW QUESTION 78
- (Exam Topic 5)
Which of the following is a common technology for visual monitoring?

A. Closed circuit television
B. Open circuit television
C. Blocked video
D. Local video

Answer: A

Explanation:
Reference: https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/

NEW QUESTION 83
- (Exam Topic 5)
Using the Transport Layer Security (TLS) protocol enables a client in a network to be:

A. Provided with a digital signature
B. Assured of the server's identity
C. Identified by a network
D. Registered by the server

Answer: B

Explanation:
Reference: https://ukdiss.com/examples/tls.php

NEW QUESTION 84
- (Exam Topic 5)
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 asset

Answer: D

NEW QUESTION 86
- (Exam Topic 5)
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 sponsorship from executive management

Answer: B

NEW QUESTION 89
- (Exam Topic 5)
Which of the following provides an independent assessment of a vendor's internal security controls and overall posture?

A. Alignment with business goals
B. ISO27000 accreditation
C. PCI attestation of compliance
D. Financial statements

Answer: B

NEW QUESTION 92
- (Exam Topic 5)
The rate of change in technology increases the importance of:

A. Outsourcing the IT functions.
B. Understanding user requirements.
C. Hiring personnel with leading edge skills.
D. Implementing and enforcing good processes.

Answer: D

NEW QUESTION 96
- (Exam Topic 5)
A CISO wants to change the defense strategy to ward off attackers. To accomplish this the CISO is looking to a strategy where attackers are lured into a zone of a safe network where attackers can be monitored, controlled, quarantined, or eradicated.

A. Moderate investment
B. Passive monitoring
C. Integrated security controls
D. Dynamic deception

Answer: D

NEW QUESTION 97
- (Exam Topic 5)
The ability to demand the implementation and management of security controls on third parties providing services to an organization is

A. Security Governance
B. Compliance management
C. Vendor management
D. Disaster recovery

Answer: C

NEW QUESTION 98
- (Exam Topic 5)
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
Which of the following frameworks and standards will BEST fit the organization as a baseline for their security program?

A. NIST and Privacy Regulations
B. ISO 27000 and Payment Card Industry Data Security Standards
C. NIST and data breach notification laws
D. ISO 27000 and Human resources best practices

Answer: B

NEW QUESTION 101
- (Exam Topic 5)

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years. This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?

A. International encryption restrictions
B. Compliance to Payment Card Industry (PCI) data security standards
C. Compliance with local government privacy laws
D. Adherence to local data breach notification laws

Answer: B

NEW QUESTION 106
- (Exam Topic 5)
The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

A. Security certification
B. Security system analysis
C. Security accreditation
D. Alignment with business practices and goals.

Answer: C

NEW QUESTION 111
- (Exam Topic 5)
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

NEW QUESTION 113
- (Exam Topic 5)
Which of the following is a primary method of applying consistent configurations to IT systems?

A. Audits
B. Administration
C. Patching
D. Templates

Answer: C

NEW QUESTION 118
- (Exam Topic 5)
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. Security practices not in alignment with ISO 27000 frameworks
D. Lack of technical controls when dealing with credit card data

Answer: A

NEW QUESTION 122
- (Exam Topic 5)
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.
During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical aspect of the team’s activities?

A. Regular communication of incident status to executives
B. Eradication of malware and system restoration
C. Determination of the attack source
D. Preservation of information

Answer: D

NEW QUESTION 125
- (Exam Topic 5)

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. Create timelines for mitigation
B. Develop a cost-benefit analysis
C. Calculate annual loss expectancy
D. Create a detailed technical executive summary

Answer: B

NEW QUESTION 130
- (Exam Topic 5)
Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
Symmetric encryption in general is preferable to asymmetric encryption when:

A. The number of unique communication links is large
B. The volume of data being transmitted is small
C. The speed of the encryption / deciphering process is essential
D. The distance to the end node is farthest away

Answer: C

NEW QUESTION 135
- (Exam Topic 5)
Which of the following is an accurate description of a balance sheet?

A. The percentage of earnings that are retained by the organization for reinvestment in the business
B. The details of expenses and revenue over a long period of time
C. A summarized statement of all assets and liabilities at a specific point in time
D. A review of regulations and requirements impacting the business from a financial perspective

Answer: C

NEW QUESTION 139
- (Exam Topic 5)
Where does bottom-up financial planning primarily gain information for creating budgets?

A. By adding all capital and operational costs from the prior budgetary cycle, and determining potential financial shortages
B. By reviewing last year’s program-level costs and adding a percentage of expected additional portfolio costs
C. By adding the cost of all known individual tasks and projects that are planned for the next budgetary cycle
D. By adding all planned operational expenses per quarter then summarizing them in a budget request

Answer: D

NEW QUESTION 143
- (Exam Topic 5)
Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

A. They need to use Nessus.
B. They can implement Wireshark.
C. Snort is the best tool for their situation.
D. They could use Tripwire.

Answer: C

Explanation:
Reference: https://searchnetworking.techtarget.com/definition/Snort

NEW QUESTION 145
- (Exam Topic 5)
What is meant by password aging?

A. An expiration date set for passwords
B. A Single Sign-On requirement
C. Time in seconds a user is allocated to change a password
D. The amount of time it takes for a password to activate

Answer: C

Explanation:
Reference: https://medical-dictionary.thefreedictionary.com/password+ageing

NEW QUESTION 150
- (Exam Topic 5)
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.
What action should you take FIRST?

A. Destroy the repository of stolen data
B. Contact your local law enforcement agency
C. Consult with other C-Level executives to develop an action plan
D. Contract with a credit reporting company for paid monitoring services for affected customers

Answer: C

NEW QUESTION 154
- (Exam Topic 5)
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. Scope of the project
B. Training of the personnel on the project
C. Timeline of the project milestones
D. Vendor for the project

Answer: A

NEW QUESTION 157
- (Exam Topic 5)
Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?

A. Security regulations
B. Asset classification
C. Information security policy
D. Data classification

Answer: C

NEW QUESTION 162
- (Exam Topic 5)
Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan
B. Iris scan
C. Signature kinetics scan
D. Retinal scan

Answer: D

NEW QUESTION 167
- (Exam Topic 5)
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.
What phase of the response provides measures to reduce the likelihood of an incident from recurring?

A. Response
B. Investigation
C. Recovery
D. Follow-up

Answer: D

NEW QUESTION 172
- (Exam Topic 5)
As the Chief Information Security Officer, you are performing an assessment of security posture to understand what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows to detect and actively stop vulnerability exploits and attacks?

A. Gigamon
B. Intrusion Prevention System
C. Port Security
D. Anti-virus

Answer: B

Explanation:
Reference: https://searchsecurity.techtarget.com/definition/intrusion-prevention

NEW QUESTION 177
- (Exam Topic 4)
In terms of supporting a forensic investigation, it is now imperative that managers, first-responders, etc., accomplish the following actions to the computer under investigation:

A. Secure the area and shut-down the computer until investigators arrive
B. Secure the area and attempt to maintain power until investigators arrive
C. Immediately place hard drive and other components in an anti-static bag
D. Secure the area.

Answer: B

NEW QUESTION 181
- (Exam Topic 4)
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: A

NEW QUESTION 182
- (Exam Topic 4)
The process of creating a system which divides documents based on their security level to manage access to private data is known as

A. security coding
B. data security system
C. data classification
D. privacy protection

Answer: C

NEW QUESTION 187
- (Exam Topic 4)
A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?

A. non-repudiation
B. conflict resolution
C. strong authentication
D. digital rights management

Answer: A

NEW QUESTION 188
- (Exam Topic 4)
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

A. Shared key
B. Asynchronous
C. Open
D. None

Answer: A

NEW QUESTION 193
- (Exam Topic 4)
As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.
* 1.Covering tracks
* 2.Scanning and enumeration
* 3.Maintaining Access
* 4.Reconnaissance
* 5. Gaining Access

A. 4, 2, 5, 3, 1
B. 2, 5, 3, 1, 4
C. 4, 5, 2, 3, 1
D. 4, 3, 5, 2, 1

Answer: A

NEW QUESTION 196
- (Exam Topic 4)
What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

A. Traffic Analysis
B. Deep-Packet inspection
C. Packet sampling
D. Heuristic analysis

Answer: B

NEW QUESTION 199
- (Exam Topic 4)
Which of the following statements about Encapsulating Security Payload (ESP) is true?

A. It is an IPSec protocol.
B. It is a text-based communication protocol.
C. It uses TCP port 22 as the default port and operates at the application layer.
D. It uses UDP port 22

Answer: A

NEW QUESTION 200
- (Exam Topic 4)
What is the FIRST step in developing the vulnerability management program?

A. Baseline the Environment
B. Maintain and Monitor
C. Organization Vulnerability
D. Define Policy

Answer: A

NEW QUESTION 204
- (Exam Topic 3)
The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong? (choose the BEST answer):

A. Failed to identify all stakeholders and their needs
B. Deployed the encryption solution in an inadequate manner
C. Used 1024 bit encryption when 256 bit would have sufficed
D. Used hardware encryption instead of software encryption

Answer: A

NEW QUESTION 209
- (Exam Topic 3)
Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

A. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
B. Create separate controls for the business units based on the types of business and functions they perform
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: C

NEW QUESTION 213
- (Exam Topic 3)
What oversight should the information security team have in the change management process for application security?

A. Information security should be informed of changes to applications only
B. Development team should tell the information security team about any application security flaws
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 aware of all application changes and work with developers before changes are deployed in production

Answer: C

NEW QUESTION 217
- (Exam Topic 3)
Which of the following methodologies references the recommended industry standard that Information security project managers should follow?

A. The Security Systems Development Life Cycle
B. The Security Project And Management Methodology
C. Project Management System Methodology

D. Project Management Body of Knowledge

Answer: D

NEW QUESTION 218
- (Exam Topic 3)
Which of the following are not stakeholders of IT security projects?

A. Board of directors
B. Third party vendors
C. CISO
D. Help Desk

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
When selecting a security solution with reoccurring maintenance costs after the first year, the CISO should: (choose the BEST answer)

A. The CISO should cut other essential programs to ensure the new solution’s continued use
B. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution’s continued use
C. Defer selection until the market improves and cash flow is positive
D. Implement the solution and ask for the increased operating cost budget when it is time

Answer: B

NEW QUESTION 226
- (Exam Topic 3)
Which of the following represents the BEST method of ensuring security program alignment to business needs?

A. Create a comprehensive security awareness program and provide success metrics to business units
B. Create security consortiums, such as strategic security planning groups, that include business unit participation
C. Ensure security implementations include business unit testing and functional validation prior to production rollout
D. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role

Answer: B

NEW QUESTION 231
- (Exam Topic 3)
The ultimate goal of an IT security projects is:

A. Increase stock value
B. Complete security
C. Support business requirements
D. Implement information security policies

Answer: C

NEW QUESTION 234
- (Exam Topic 3)
An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents. Which of the following would be considered a MAJOR constraint for the project?

A. Time zone differences
B. Compliance to local hiring laws
C. Encryption import/export regulations
D. Local customer privacy laws

Answer: C

NEW QUESTION 235
- (Exam Topic 3)
Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed. What can be done to ensure that security is addressed cost effectively?

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

Answer: D

NEW QUESTION 237
- (Exam Topic 2)
An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to

determine impact to the company for each application. What should be the NEXT step?

A. Determine the annual loss expectancy (ALE)
B. Create a crisis management plan
C. Create technology recovery plans
D. Build a secondary hot site

Answer: C

NEW QUESTION 241
- (Exam Topic 2)
Dataflow diagrams are used by IT auditors to:

A. Order data hierarchically.
B. Highlight high-level data definitions.
C. Graphically summarize data paths and storage processes.
D. Portray step-by-step details of data generation.

Answer: C

NEW QUESTION 245
- (Exam Topic 2)
Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

A. International Organization for Standardization 27001
B. National Institute of Standards and Technology Special Publication SP 800-12
C. Request For Comment 2196
D. National Institute of Standards and Technology Special Publication SP 800-26

Answer: A

NEW QUESTION 248
- (Exam Topic 2)
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

A. Security Administrators
B. Internal/External Audit
C. Risk Management
D. Security Operations

Answer: B

NEW QUESTION 250
- (Exam Topic 2)
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. Database Administration
C. Information Security
D. Compliance

Answer: C

NEW QUESTION 252
- (Exam Topic 2)
Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

A. Control Objective for Information Technology (COBIT)
B. Committee of Sponsoring Organizations (COSO)
C. Payment Card Industry (PCI)
D. Information Technology Infrastructure Library (ITIL)

Answer: A

NEW QUESTION 255
- (Exam Topic 2)
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. Business Continuity plan
C. Disaster recovery plan
D. Damage control plan

Answer: C

NEW QUESTION 258
- (Exam Topic 2)
A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?

A. Have internal audit conduct another audit to see what has changed.
B. Contract with an external audit company to conduct an unbiased audit
C. Review the recommendations and follow up to see if audit implemented the changes
D. Meet with audit team to determine a timeline for corrections

Answer: C

NEW QUESTION 261
- (Exam Topic 2)
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 periodic examination of access rights
C. Failure to notify police of an attempted intrusion
D. Lack of reporting of a successful denial of service attack on the network.

Answer: A

NEW QUESTION 263
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 712-50 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 712-50 Product From:

https://www.2passeasy.com/dumps/712-50/

Money Back Guarantee

712-50 Practice Exam Features:

* 712-50 Questions and Answers Updated Frequently

* 712-50 Practice Questions Verified by Expert Senior Certified Staff

* 712-50 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 712-50 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year