EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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)
The primary responsibility for assigning entitlements to a network share lies with which role?

A. CISO
B. Data owner
C. Chief Information Officer (CIO)
D. Security system administrator

Answer: B

Explanation:
Reference: https://resources.infosecinstitute.com/certification/data-and-system-ownership/

NEW QUESTION 4
- (Exam Topic 6)
A Security Operations Manager is finding it difficult to maintain adequate staff levels to monitor security operations during off-hours. To reduce the impact of staff shortages and increase coverage during off-hours, the SecOps manager is considering outsourcing off-hour coverage.
What Security Operations Center (SOC) model does this BEST describe?

A. Virtual SOC
B. In-house SOC
C. Security Network Operations Center (SNOC)
D. Hybrid SOC

Answer: A

Explanation:
Reference:
https://www.techtarget.com/searchsecurity/tip/Benefits-of-virtual-SOCs-Enterprise-run-vs-fully-managed

NEW QUESTION 5
- (Exam Topic 6)
What organizational structure combines the functional and project structures to create a hybrid of the two?

A. Traditional
B. Composite
C. Project
D. Matrix

Answer: D

Explanation:
Reference: https://www.knowledgehut.com/tutorials/project-management/organization-structures

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 6)
When managing a project, the MOST important activity in managing the expectations of stakeholders is:

A. To force stakeholders to commit ample resources to support the project
B. To facilitate proper communication regarding outcomes
C. To assure stakeholders commit to the project start and end dates in writing
D. To finalize detailed scope of the project at project initiation

Answer: B

Explanation:
Reference:
https://www.greycampus.com/blog/project-management/stakeholder-management-what-is-it-and-why-is-it-so-im

NEW QUESTION 9
- (Exam Topic 6)
XYZ is a publicly-traded software development company.
Who is ultimately accountable to the shareholders in the event of a cybersecurity breach?

A. Chief Financial Officer (CFO)
B. Chief Software Architect (CIO)
C. CISO
D. Chief Executive Officer (CEO)

Answer: C

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

NEW QUESTION 10
- (Exam Topic 6)
In defining a strategic security plan for an organization, what should a CISO first analyze?

A. Reach out to a business similar to yours and ask for their plan
B. Set goals that are difficult to attain to drive more productivity
C. Review business acquisitions for the past 3 years
D. Analyze the broader organizational strategic plan

Answer: D

Explanation:
Reference: https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/

NEW QUESTION 10
- (Exam Topic 6)
ABC Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame. You would like to implement key performance indicators to mitigate the risk.
Which metric would meet the requirement?

A. Number of times third parties access critical information systems
B. Number of systems with known vulnerabilities
C. Number of users with elevated privileges
D. Number of websites with weak or misconfigured certificates

Answer: C

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 16
- (Exam Topic 2)
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. Anti-Spam controls.
C. Security Awareness Program.
D. Identity and Access Management Program.

Answer: C

NEW QUESTION 20
- (Exam Topic 2)
When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

A. Daily
B. Hourly
C. Weekly
D. Monthly

Answer: A

NEW QUESTION 24
- (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 26
- (Exam Topic 2)
Control Objectives for Information and Related Technology (COBIT) is which of the following?

A. An Information Security audit standard
B. An audit guideline for certifying secure systems and controls
C. A framework for Information Technology management and governance
D. A set of international regulations for Information Technology governance

Answer: C

NEW QUESTION 30
- (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 32
- (Exam Topic 2)
To have accurate and effective information security policies how often should the CISO review the organization policies?

A. Every 6 months
B. Quarterly
C. Before an audit
D. At least once a year

Answer: D

NEW QUESTION 37
- (Exam Topic 1)
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. Security incident disclosure
D. Special circumstance disclosure

Answer: A

NEW QUESTION 38
- (Exam Topic 1)
What two methods are used to assess risk impact?

A. Cost and annual rate of expectance
B. Subjective and Objective
C. Qualitative and percent of loss realized
D. Quantitative and qualitative

Answer: D

NEW QUESTION 43
- (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 45
- (Exam Topic 1)
Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

A. Security officer
B. Data owner
C. Vulnerability engineer
D. System administrator

Answer: D

NEW QUESTION 49
- (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 50
- (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 51
- (Exam Topic 1)
What is a difference from the list below between quantitative and qualitative Risk Assessment?

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

B. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
C. Qualitative risk assessments map to business objectives
D. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Answer: A

NEW QUESTION 52
- (Exam Topic 1)
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: B

NEW QUESTION 56
- (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 60
- (Exam Topic 1)
You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

A. Controlled mitigation effort
B. Risk impact comparison
C. Relative likelihood of event
D. Comparative threat analysis

Answer: C

NEW QUESTION 63
- (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 67
- (Exam Topic 1)
An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

A. A high threat environment
B. A low risk tolerance environment
C. I low vulnerability environment
D. A high risk tolerance environment

Answer: D

NEW QUESTION 68
- (Exam Topic 1)
Risk is defined as:

A. Threat times vulnerability divided by control
B. Advisory plus capability plus vulnerability
C. Asset loss times likelihood of event
D. Quantitative plus qualitative impact

Answer: A

NEW QUESTION 69
- (Exam Topic 1)

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. Compliance management
D. Security awareness training

Answer: C

NEW QUESTION 72
- (Exam Topic 1)
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 Protection
B. Due Care
C. Due Compromise
D. Due process

Answer: B

NEW QUESTION 77
- (Exam Topic 1)
A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization’s need?

A. International Organization for Standardizations – 22301 (ISO-22301)
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27005 (ISO-27005)

Answer: A

NEW QUESTION 80
- (Exam Topic 1)
Credit card information, medical data, and government records are all examples of:

A. Confidential/Protected Information
B. Bodily Information
C. Territorial Information
D. Communications Information

Answer: A

NEW QUESTION 85
- (Exam Topic 1)
An organization's Information Security Policy is of MOST importance because

A. it communicates management’s commitment to protecting information resources
B. it is formally acknowledged by all employees and vendors
C. it defines a process to meet compliance requirements
D. it establishes a framework to protect confidential information

Answer: A

NEW QUESTION 90
- (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 95
- (Exam Topic 1)
Who in the organization determines access to information?

A. Legal department
B. Compliance officer
C. Data Owner
D. Information security officer

Answer: C

NEW QUESTION 100
- (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 103
- (Exam Topic 6)
As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity.
The performance quality audit activity is done in what project management process group?

A. Executing
B. Controlling
C. Planning
D. Closing

Answer: A

Explanation:
Reference:
https://blog.masterofproject.com/executing-process-group-project-management/#:~:text=Executing%20Process

NEW QUESTION 104
- (Exam Topic 6)
As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand.
Which is the BEST type of risk that defines this event?

A. Compliance Risk
B. Reputation Risk
C. Operational Risk
D. Strategic Risk

Answer: B

NEW QUESTION 105
- (Exam Topic 5)
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. Enable monitoring on the VPN for suspicious activity
C. Force a change of all passwords
D. Block access to the Employee-Self Service application via VPN

Answer: D

NEW QUESTION 106
- (Exam Topic 5)
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 area. Which type of attack did the consultant perform?

A. Shoulder surfing
B. Tailgating
C. Social engineering
D. Mantrap

Answer: B

NEW QUESTION 110
- (Exam Topic 5)
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

A. Video surveillance

B. Mantrap
C. Bollards
D. Fence

Answer: D

NEW QUESTION 115
- (Exam Topic 5)
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

NEW QUESTION 119
- (Exam Topic 5)
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. Management
B. Operational
C. Technical
D. Administrative

Answer: B

NEW QUESTION 120
- (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 125
- (Exam Topic 5)
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. Validate the effectiveness of current controls
B. Create detailed remediation funding and staffing plans
C. Report the audit findings and remediation status to business stake holders
D. Review security procedures to determine if they need modified according to findings

Answer: C

NEW QUESTION 129
- (Exam Topic 5)
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.
After determining the audit findings are accurate, which of the following is the MOST logical next activity?

A. Begin initial gap remediation analyses
B. Review the security organization’s charter
C. Validate gaps with the Information Technology team
D. Create a briefing of the findings for executive management

Answer: A

NEW QUESTION 130
- (Exam Topic 5)
The formal certification and accreditation process has four primary steps, what are they?

A. Evaluating, describing, testing and authorizing
B. Evaluating, purchasing, testing, authorizing
C. Auditing, documenting, verifying, certifying
D. Discovery, testing, authorizing, certifying

Answer: A

NEW QUESTION 133
- (Exam Topic 5)
Which of the following defines the boundaries and scope of a risk assessment?

A. The risk assessment schedule
B. The risk assessment framework
C. The risk assessment charter
D. The assessment context

Answer: B

Explanation:
Reference: https://cfocussoftware.com/risk-management-framework/know-your-boundary/

NEW QUESTION 134
- (Exam Topic 5)
The primary purpose of a risk register is to:

A. Maintain a log of discovered risks
B. Track individual risk assessments
C. Develop plans for mitigating identified risks
D. Coordinate the timing of scheduled risk assessments

Answer: A

Explanation:
Reference: https://sitemate.com/us/resources/articles/safety/purpose-of-a-risk-register/

NEW QUESTION 138
- (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 139
- (Exam Topic 5)
As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

A. Recovery Point Objective (RPO)
B. Disaster Recovery Plan
C. Recovery Time Objective (RTO)
D. Business Continuity Plan

Answer: D

Explanation:
Reference: https://www.resolver.com/resource/bcdr-metrics-that-matter/

NEW QUESTION 143
- (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 145
- (Exam Topic 5)
If the result of an NPV is positive, then the project should be selected. The net present value shows the present value of the project, based on the decisions taken

for its selection. What is the net present value equal to?

A. Net profit – per capita income
B. Total investment – Discounted cash
C. Average profit – Annual investment
D. Initial investment – Future value

Answer: C

NEW QUESTION 148
- (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 150
- (Exam Topic 5)
The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

A. Safeguard Value
B. Cost Benefit Analysis
C. Single Loss Expectancy
D. Life Cycle Loss Expectancy

Answer: B

NEW QUESTION 153
- (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.
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. Security Guards posted outside the Data Center
B. Data Loss Prevention (DLP)
C. Rigorous syslog reviews
D. Intrusion Detection Systems (IDS)

Answer: B

NEW QUESTION 158
- (Exam Topic 5)
Which of the following terms is used to describe countermeasures implemented to minimize risks to physical property, information, and computing systems?

A. Security frameworks
B. Security policies
C. Security awareness
D. Security controls

Answer: D

Explanation:
Reference: https://www.ibm.com/cloud/learn/security-controls

NEW QUESTION 160
- (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 162
- (Exam Topic 5)
Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?

A. ITIL
B. Privacy Act
C. Sarbanes Oxley
D. PCI-DSS

Answer: B

NEW QUESTION 166
- (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 correctly aligns with the company goals and the scope of the project is correct. What is the NEXT step?

A. Review time schedules
B. Verify budget
C. Verify resources
D. Verify constraints

Answer: C

NEW QUESTION 168
- (Exam Topic 5)
Smith, the project manager for a larger multi-location firm, is leading a software project team that has 18
members, 5 of which are assigned to testing. Due to recent recommendations by an organizational quality audit team, the project manager is convinced to add a quality professional to lead to test team at additional cost to the project.
The project manager is aware of the importance of communication for the success of the project and takes the step of introducing additional communication channels, making it more complex, in order to assure quality levels of the project. What will be the first project management document that Smith should change in order to accommodate additional communication channels?

A. WBS document
B. Scope statement
C. Change control document
D. Risk management plan

Answer: A

NEW QUESTION 171
- (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 172
- (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 173

- (Exam Topic 5)
Which of the following would negatively impact a log analysis of a multinational organization?

A. Centralized log management
B. Encrypted log files in transit
C. Each node set to local time
D. Log aggregation agent each node

Answer: D

NEW QUESTION 178
- (Exam Topic 5)
Which of the following best describes an access control process that confirms the identity of the entity seeking access to a logical or physical area?

A. Identification
B. Authorization
C. Authentication
D. Accountability

Answer: B

NEW QUESTION 181
- (Exam Topic 4)
Which of the following is a symmetric encryption algorithm?

A. 3DES
B. MD5
C. ECC
D. RSA

Answer: A

NEW QUESTION 184
- (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 186
- (Exam Topic 4)
Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

A. Trusted and untrusted networks
B. Type of authentication
C. Storage encryption
D. Log retention

Answer: A

NEW QUESTION 190
- (Exam Topic 4)
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 need to change accounting periods on a regular basis.
B. The requirement to post entries for a closed accounting period.
C. The need to create and modify the chart of accounts and its allocations.
D. The lack of policies and procedures for the proper segregation of duties.

Answer: D

NEW QUESTION 195
- (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 197
- (Exam Topic 4)
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. Enterprise Risk Assessment
B. Disaster recovery strategic plan
C. Business continuity plan
D. Application mapping document

Answer: B

NEW QUESTION 200
- (Exam Topic 4)
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. Containment
B. Recovery
C. Identification
D. Eradication

Answer: D

NEW QUESTION 201
- (Exam Topic 3)
An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in sever revenue disruptions. Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

A. The CISO
B. Audit and Compliance
C. The CFO
D. The business owner

Answer: D

NEW QUESTION 202
- (Exam Topic 3)
As the CISO for your company you are accountable for the protection of information resources commensurate with:

A. Customer demand
B. Cost and time to replace
C. Insurability tables
D. Risk of exposure

Answer: D

NEW QUESTION 205
- (Exam Topic 3)
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 asset management processes
B. Lack of change management processes
C. Lack of hardening standards
D. Lack of proper access controls

Answer: B

NEW QUESTION 210
- (Exam Topic 3)
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. Work with the IT group and tell them to put IPS in-line and say it won’t cause any network impact
B. Explain to the IT group that the IPS won’t cause any network impact because it will fail open
C. 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
D. 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

Answer: D

NEW QUESTION 213
- (Exam Topic 3)

Which of the following represents the best method of ensuring business unit alignment with security program requirements?

A. Provide clear communication of security requirements throughout the organization
B. Demonstrate executive support with written mandates for security policy adherence
C. Create collaborative risk management approaches within the organization
D. Perform increased audits of security processes and procedures

Answer: C

NEW QUESTION 215
- (Exam Topic 3)
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

NEW QUESTION 217
- (Exam Topic 3)
A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?

A. The software license expiration is probably out of synchronization with other software licenses
B. The project was initiated without an effort to get support from impacted business units in the organization
C. The software is out of date and does not provide for a scalable solution across the enterprise
D. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
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. Ineffective configuration management controls
B. Lack of change management controls
C. Lack of version/source controls
D. High turnover in the application development department

Answer: C

NEW QUESTION 224
- (Exam Topic 3)
A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets. This demonstrates which of the following principles?

A. Security alignment to business goals
B. Regulatory compliance effectiveness
C. Increased security program presence
D. Proper organizational policy enforcement

Answer: A

NEW QUESTION 226
- (Exam Topic 3)
An example of professional unethical behavior is:

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

Answer: C

NEW QUESTION 227
- (Exam Topic 3)
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. Intrusion Detection System (IDS), firewall, switch, syslog
C. Security Incident Event Management (SIEM), IDS, router, syslog
D. SIEM, IDS, firewall, VMS

Answer: D

NEW QUESTION 229
- (Exam Topic 3)
Which of the following can the company implement in order to avoid this type of security issue in the future?

A. Network based intrusion detection systems
B. A security training program for developers
C. A risk management process
D. A audit management process

Answer: B

NEW QUESTION 233
- (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 236
- (Exam Topic 3)
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. it comes in at or below the expenditures planned for in the baseline budget
D. the deliverables are accepted by the key stakeholders

Answer: D

NEW QUESTION 239
- (Exam Topic 3)
When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization. Which example below is the MOST creative way to maintain a strong security posture during these difficult times?

A. Download open source security tools and deploy them on your production network
B. Download trial versions of commercially available security tools and deploy on your production network
C. Download open source security tools from a trusted site, test, and then deploy on production network
D. Download security tools from a trusted source and deploy to production network

Answer: C

NEW QUESTION 244
- (Exam Topic 3)
How often should the SSAE16 report of your vendors be reviewed?

A. Quarterly
B. Semi-annually
C. Annually
D. Bi-annually

Answer: C

NEW QUESTION 248
- (Exam Topic 3)
Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

A. Terms and Conditions
B. Service Level Agreements (SLA)
C. Statement of Work
D. Key Performance Indicators (KPI)

Answer: B

NEW QUESTION 250
- (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 255
- (Exam Topic 3)
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. Quarterly
B. Semi-annually
C. Bi-annually
D. Annually

Answer: D

NEW QUESTION 259
- (Exam Topic 3)
A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

A. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
B. A clear set of security policies and procedures that are more concept-based than controls-based
C. A complete inventory of Information Technology assets including infrastructure, networks, applications and data
D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

Answer: D

NEW QUESTION 261
- (Exam Topic 3)
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. Once the agreement has been signed and the security vendor states that they will need 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

NEW QUESTION 262
- (Exam Topic 2)
Which of the following activities must be completed BEFORE you can calculate risk?

A. Determining the likelihood that vulnerable systems will be attacked by specific threats
B. Calculating the risks to which assets are exposed in their current setting
C. Assigning a value to each information asset
D. Assessing the relative risk facing the organization’s information assets

Answer: C

NEW QUESTION 264
- (Exam Topic 2)
During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

A. Identify and evaluate the existing controls.
B. Disclose the threats and impacts to management.
C. Identify information assets and the underlying systems.
D. Identify and assess the risk assessment process used by management.

Answer: A

NEW QUESTION 267
- (Exam Topic 2)
The regular review of a firewall ruleset is considered a

A. Procedural control
B. Organization control
C. Technical control
D. Management control

Answer: A

NEW QUESTION 269

- (Exam Topic 2)
Which of the following activities results in change requests?

A. Preventive actions
B. Inspection
C. Defect repair
D. Corrective actions

Answer: C

NEW QUESTION 271
- (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 276
- (Exam Topic 2)
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. Systems logs
B. Hardware error reports
C. Utilization reports
D. Availability reports

Answer: D

NEW QUESTION 279
- (Exam Topic 2)
Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

A. Single Loss Expectancy (SLE)
B. Exposure Factor (EF)
C. Annualized Rate of Occurrence (ARO)
D. Temporal Probability (TP)

Answer: C

NEW QUESTION 283
......

Relate Links

100% Pass Your 712-50 Exam with Exambible Prep Materials

https://www.exambible.com/712-50-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/