EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (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 2
- (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 3
- (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 4
- (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 5
- (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 6
- (Exam Topic 6)
Of the following types of SOCs (Security Operations Centers), which one would be MOST likely used if the CISO has decided to outsource the infrastructure and administration of it?

A. Virtual
B. Dedicated
C. Fusion
D. Command

Answer: A

Explanation:
Reference: https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (Exam Topic 2)
When you develop your audit remediation plan what is the MOST important criteria?

A. To remediate half of the findings before the next audit.
B. To remediate all of the findings before the next audit.
C. To validate that the cost of the remediation is less than the risk of the finding.
D. To validate the remediation process with the auditor.

Answer: C

NEW QUESTION 10
- (Exam Topic 2)
How often should an environment be monitored for cyber threats, risks, and exposures?

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

Answer: D

NEW QUESTION 13
- (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 14
- (Exam Topic 2)
A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

A. The auditors have not followed proper auditing processes
B. The CIO of the organization disagrees with the finding
C. The risk tolerance of the organization permits this risk
D. The organization has purchased cyber insurance

Answer: C

NEW QUESTION 16
- (Exam Topic 1)
An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?

A. Determine the risk tolerance
B. Perform an asset classification
C. Create an architecture gap analysis
D. Analyze existing controls on systems

Answer: B

NEW QUESTION 20
- (Exam Topic 1)
When managing the security architecture for your company you must consider:

A. Security and IT Staff size
B. Company Values
C. Budget
D. All of the above

Answer: D

NEW QUESTION 23
- (Exam Topic 1)
You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

A. Risk Avoidance
B. Risk Acceptance
C. Risk Transfer
D. Risk Mitigation

Answer: C

NEW QUESTION 26
- (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 27
- (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)
A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

A. Enforce the existing security standards and do not allow the deployment of the new technology.
B. Amend the standard to permit the deployment.
C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Answer: C

NEW QUESTION 36
- (Exam Topic 1)
According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

A. Susceptibility to attack, mitigation response time, and cost
B. Attack vectors, controls cost, and investigation staffing needs
C. Vulnerability exploitation, attack recovery, and mean time to repair
D. Susceptibility to attack, expected duration of attack, and mitigation availability

Answer: A

NEW QUESTION 41
- (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 42
- (Exam Topic 1)
After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

A. Risk Tolerance
B. Qualitative risk analysis
C. Risk Appetite
D. Quantitative risk analysis

Answer: D

NEW QUESTION 47
- (Exam Topic 1)
What role should the CISO play in properly scoping a PCI environment?

A. Validate the business units' suggestions as to what should be included in the scoping process
B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment
C. Ensure internal scope validation is completed and that an assessment has been done to discover all credit card data
D. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope

Answer: C

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 53
- (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 58
- (Exam Topic 1)
Which of the following is MOST likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

Answer: C

NEW QUESTION 62
- (Exam Topic 1)
You have implemented a new security control. Which of the following risk strategy options have you engaged in?

A. Risk Avoidance
B. Risk Acceptance
C. Risk Transfer
D. Risk Mitigation

Answer: D

NEW QUESTION 63
- (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 64
- (Exam Topic 1)
The single most important consideration to make when developing your security program, policies, and processes is:

A. Budgeting for unforeseen data compromises
B. Streamlining for efficiency
C. Alignment with the business
D. Establishing your authority as the Security Executive

Answer: C

NEW QUESTION 68
- (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 71
- (Exam Topic 1)
Which of the following is a critical operational component of an Incident Response Program (IRP)?

A. Weekly program budget reviews to ensure the percentage of program funding remains constant.
B. Annual review of program charters, policies, procedures and organizational agreements.
C. Daily monitoring of vulnerability advisories relating to your organization's deployed technologies.
D. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization

Answer: C

NEW QUESTION 74
- (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 78
- (Exam Topic 1)
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 security awareness program
B. Lack of a formal security policy governance process
C. Lack of formal definition of roles and responsibilities
D. Lack of a formal risk management policy

Answer: B

NEW QUESTION 79
- (Exam Topic 1)
The exposure factor of a threat to your organization is defined by?

A. Asset value times exposure factor
B. Annual rate of occurrence
C. Annual loss expectancy minus current cost of controls
D. Percentage of loss experienced due to a realized threat event

Answer: D

NEW QUESTION 82
- (Exam Topic 1)
The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope
B. Getting authority to operate the system from executive management
C. Changing the default passwords
D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

NEW QUESTION 83
- (Exam Topic 1)
What is the MAIN reason for conflicts between Information Technology and Information Security programs?

A. Technology governance defines technology policies and standards while security governance does not.
B. Security governance defines technology best practices and Information Technology governance does not.
C. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
D. The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.

Answer: D

NEW QUESTION 87
- (Exam Topic 1)
Regulatory requirements typically force organizations to implement

A. Mandatory controls
B. Discretionary controls
C. Optional controls
D. Financial controls

Answer: A

NEW QUESTION 91
- (Exam Topic 1)
Which of the following has the GREATEST impact on the implementation of an information security governance model?

A. Organizational budget
B. Distance between physical locations
C. Number of employees
D. Complexity of organizational structure

Answer: D

NEW QUESTION 94

- (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 99
- (Exam Topic 1)
Which of the following provides an audit framework?

A. Control Objectives for IT (COBIT)
B. Payment Card Industry-Data Security Standard (PCI-DSS)
C. International Organization Standard (ISO) 27002
D. National Institute of Standards and Technology (NIST) SP 800-30

Answer: A

NEW QUESTION 103
- (Exam Topic 1)
What is the relationship between information protection and regulatory compliance?

A. That all information in an organization must be protected equally.
B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
C. That the protection of some information such as National ID information is mandated by regulation andother information such as trade secrets are protected based on business need.
D. There is no relationship between the two.

Answer: C

NEW QUESTION 105
- (Exam Topic 1)
In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

A. High risk environments 6 months, low risk environments 12 months
B. Every 12 months
C. Every 18 months
D. Every six months

Answer: B

NEW QUESTION 109
- (Exam Topic 6)
When information security falls under the Chief Information Officer (CIO), what is their MOST essential role?

A. Oversees the organization's day-to-day operations, creating the policies and strategies that govern operations
B. Enlisting support from key executives the information security program budget and policies
C. Charged with developing and implementing policies designed to protect employees and customers' data from unauthorized access
D. Responsible for the success or failure of the IT organization and setting strategic direction

Answer: D

Explanation:
Reference: https://www.investopedia.com/terms/c/cio.asp

NEW QUESTION 111
- (Exam Topic 6)
To make sure that the actions of all employees, applications, and systems follow the organization's rules and regulations can BEST be described as which of the following?

A. Compliance management
B. Asset management
C. Risk management
D. Security management

Answer: D

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

NEW QUESTION 115
- (Exam Topic 6)
What is an approach to estimating the strengths and weaknesses of alternatives used to determine options, which provide the BEST approach to achieving

benefits while preserving savings called?

A. Business Impact Analysis
B. Economic Impact analysis
C. Return on Investment
D. Cost-benefit analysis

Answer: D

Explanation:
Reference: https://artsandculture.google.com/entity/cost%E2%80%93benefit-analysis/m020w0x?hl=en

NEW QUESTION 118
- (Exam Topic 6)
When evaluating a Managed Security Services Provider (MSSP), which service(s) is/are most important:

A. Patch management
B. Network monitoring
C. Ability to provide security services tailored to the business' needs
D. 24/7 tollfree number

Answer: C

Explanation:
Reference: https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps

NEW QUESTION 122
- (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 123
- (Exam Topic 6)
A CISO must conduct risk assessments using a method where the Chief Financial Officer (CFO) receives impact data in financial terms to use as input to select the proper level of coverage in a new cybersecurity insurance policy.
What is the MOST effective method of risk analysis to provide the CFO with the information required?

A. Conduct a quantitative risk assessment
B. Conduct a hybrid risk assessment
C. Conduct a subjective risk assessment
D. Conduct a qualitative risk assessment

Answer: D

NEW QUESTION 127
- (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 131
- (Exam Topic 5)
What are the three stages of an identity and access management system?

A. Authentication, Authorize, Validation
B. Provision, Administration, Enforcement
C. Administration, Validation, Protect
D. Provision, Administration, Authentication

Answer: A

Explanation:
Reference: https://digitalguardian.com/blog/what-identity-and-access-management-iam

NEW QUESTION 132
- (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 136
- (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 138
- (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 142
- (Exam Topic 5)
Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

A. Segmentation controls.
B. Shadow applications.
C. Deception technology.
D. Vulnerability management.

Answer: B

NEW QUESTION 144
- (Exam Topic 5)
During the last decade, what trend has caused the MOST serious issues in relation to physical security?

A. Data is more portable due to the increased use of smartphones and tablets
B. The move from centralized computing to decentralized computing
C. Camera systems have become more economical and expanded in their use
D. The internet of Things allows easy compromise of cloud-based systems

Answer: A

NEW QUESTION 149
- (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 151
- (Exam Topic 5)

Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
What is one proven method to account for common elements found within separate regulations and/or standards?

A. Hire a GRC expert
B. Use the Find function of your word processor
C. Design your program to meet the strictest government standards
D. Develop a crosswalk

Answer: D

NEW QUESTION 152
- (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.
Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

A. Scope
B. Budget
C. Resources
D. Constraints

Answer: A

NEW QUESTION 155
- (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 159
- (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.
How can you reduce the administrative burden of distributing symmetric keys for your employer?

A. Use asymmetric encryption for the automated distribution of the symmetric key
B. Use a self-generated key on both ends to eliminate the need for distribution
C. Use certificate authority to distribute private keys
D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

Answer: A

NEW QUESTION 160
- (Exam Topic 5)
What are the primary reasons for the development of a business case for a security project?

A. To estimate risk and negate liability to the company
B. To understand the attack vectors and attack sources
C. To communicate risk and forecast resource needs
D. To forecast usage and cost per software licensing

Answer: C

NEW QUESTION 165
- (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 169
- (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 174
- (Exam Topic 5)
When updating the security strategic planning document what two items must be included?

A. Alignment with the business goals and the vision of the CIO
B. The risk tolerance of the company and the company mission statement
C. The executive summary and vision of the board of directors
D. The alignment with the business goals and the risk tolerance

Answer: D

NEW QUESTION 178
- (Exam Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

A. Controlled spear phishing campaigns
B. Password changes
C. Baselining of computer systems
D. Scanning for viruses

Answer: A

NEW QUESTION 183
- (Exam Topic 5)
When dealing with risk, the information security practitioner may choose to:

A. assign
B. transfer
C. acknowledge
D. defer

Answer: C

NEW QUESTION 188
- (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 190
- (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 193

- (Exam Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

A. Conduct background checks on individuals before hiring them
B. Develop an Information Security Awareness program
C. Monitor employee browsing and surfing habits
D. Set your firewall permissions aggressively and monitor logs regularly.

Answer: A

NEW QUESTION 196
- (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 198
- (Exam Topic 5)
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

Explanation:
Reference: https://www.investopedia.com/terms/r/revenue.asp

NEW QUESTION 203
- (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 204
- (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 206
- (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 210
- (Exam Topic 5)
Which of the following is the MOST logical method of deploying security controls within an organization?

A. Obtain funding for all desired controls and then create project plans for implementation
B. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult andcostly controls
C. Apply the least costly controls to demonstrate positive program activity
D. Obtain business unit buy-in through close communication and coordination

Answer: B

NEW QUESTION 214
- (Exam Topic 5)
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: B

NEW QUESTION 217
- (Exam Topic 5)
Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

A. Rights collision
B. Excessive privileges
C. Privilege creep
D. Least privileges

Answer: B

NEW QUESTION 219
- (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 223
- (Exam Topic 4)
Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?

A. In-line hardware keyloggers don't require physical access
B. In-line hardware keyloggers don't comply to industry regulations
C. In-line hardware keyloggers are undetectable by software
D. In-line hardware keyloggers are relatively inexpensive

Answer: C

NEW QUESTION 224
- (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 226
- (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 230
- (Exam Topic 4)
Security related breaches are assessed and contained through which of the following?

A. The IT support team.
B. A forensic analysis.
C. Incident response
D. Physical security team.

Answer: C

NEW QUESTION 235
- (Exam Topic 4)
You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

A. Execute
B. Read
C. Administrator
D. Public

Answer: D

NEW QUESTION 238
- (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 241
- (Exam Topic 3)
You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

A. Risk averse
B. Risk tolerant
C. Risk conditional
D. Risk minimal

Answer: B

NEW QUESTION 243
- (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 246
- (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 250
- (Exam Topic 3)
Your incident response plan should include which of the following?

A. Procedures for litigation
B. Procedures for reclamation
C. Procedures for classification
D. Procedures for charge-back

Answer: C

NEW QUESTION 251
- (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 256
- (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 259
- (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 264
- (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 267
- (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 272
- (Exam Topic 3)
Risk appetite is typically determined by which of the following organizational functions?

A. Security
B. Business units
C. Board of Directors
D. Audit and compliance

Answer: C

NEW QUESTION 276
- (Exam Topic 3)
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. A lack of executive presence within the security program
C. Poor alignment of the security program to business needs
D. This is normal since business units typically resist security requirements

Answer: C

NEW QUESTION 277
- (Exam Topic 3)
Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

A. Security administrators
B. Security mangers
C. Security technicians
D. Security analysts

Answer: B

NEW QUESTION 281
- (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 283
- (Exam Topic 3)
The company decides to release the application without remediating the high-risk vulnerabilities. Which of the following is the MOST likely reason for the company to release the application?

A. The company lacks a risk management process
B. The company does not believe the security vulnerabilities to be real
C. The company has a high risk tolerance
D. The company lacks the tools to perform a vulnerability assessment

Answer: C

NEW QUESTION 284
- (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 289
- (Exam Topic 3)
You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do. What is the BEST approach to handle this situation?

A. Tell the team to do their best and respond to each alert
B. Tune the sensors to help reduce false positives so the team can react better
C. Request additional resources to handle the workload
D. Tell the team to only respond to the critical and high alerts

Answer: B

NEW QUESTION 290
- (Exam Topic 3)
Which of the following is a major benefit of applying risk levels?

A. Risk management governance becomes easier since most risks remain low once mitigated
B. Resources are not wasted on risks that are already managed to an acceptable level
C. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology
D. Risk appetite can increase within the organization once the levels are understood

Answer: B

NEW QUESTION 295
- (Exam Topic 3)
Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

A. System testing
B. Risk assessment
C. Incident response
D. Planning

Answer: A

NEW QUESTION 298
- (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 299
- (Exam Topic 3)
When should IT security project management be outsourced?

A. When organizational resources are limited
B. When the benefits of outsourcing outweigh the inherent risks of outsourcing
C. On new, enterprise-wide security initiatives
D. On projects not forecasted in the yearly budget

Answer: B

NEW QUESTION 304
- (Exam Topic 3)
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

A. Alignment with the business
B. Effective use of existing technologies
C. Leveraging existing implementations
D. Proper budget management

Answer: A

NEW QUESTION 307
- (Exam Topic 2)
Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

A. Senior Executives
B. Office of the Auditor
C. Office of the General Counsel
D. All employees and users

Answer: A

NEW QUESTION 311
- (Exam Topic 2)
IT control objectives are useful to IT auditors as they provide the basis for understanding the:

A. Desired results or purpose of implementing specific control procedures.
B. The audit control checklist.
C. Techniques for securing information.

D. Security policy

Answer: A

NEW QUESTION 314
- (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 315
- (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 319
- (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 324
- (Exam Topic 2)
The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

A. Risk metrics
B. Management metrics
C. Operational metrics
D. Compliance metrics

Answer: C

NEW QUESTION 329
- (Exam Topic 2)
The amount of risk an organization is willing to accept in pursuit of its mission is known as

A. Risk mitigation
B. Risk transfer
C. Risk tolerance
D. Risk acceptance

Answer: C

NEW QUESTION 331
- (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 335
- (Exam Topic 2)
Which of the following illustrates an operational control process:

A. Classifying an information system as part of a risk assessment

B. Installing an appropriate fire suppression system in the data center
C. Conducting an audit of the configuration management process
D. Establishing procurement standards for cloud vendors

Answer: B

NEW QUESTION 340
- (Exam Topic 2)
Which represents PROPER separation of duties in the corporate environment?

A. Information Security and Identity Access Management teams perform two distinct functions
B. Developers and Network teams both have admin rights on servers
C. Finance has access to Human Resources data
D. Information Security and Network teams perform two distinct functions

Answer: D

NEW QUESTION 343
- (Exam Topic 2)
Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

A. ISO 27001
B. ISO 27002
C. ISO 27004
D. ISO 27005

Answer: D

NEW QUESTION 344
- (Exam Topic 2)
Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

A. Perform a vulnerability scan of the network
B. External penetration testing by a qualified third party
C. Internal Firewall ruleset reviews
D. Implement network intrusion prevention systems

Answer: B

NEW QUESTION 346
- (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 347
- (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 350
......

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/