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)
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)
Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?

A. Purge
B. Clear
C. Mangle
D. Destroy

Answer: B

Explanation:
Reference:
https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations

NEW QUESTION 3
- (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 4
- (Exam Topic 6)
A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

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

Answer: D

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

NEW QUESTION 5
- (Exam Topic 6)
During a cyber incident, which non-security personnel might be needed to assist the security team?

A. Threat analyst, IT auditor, forensic analyst
B. Network engineer, help desk technician, system administrator
C. CIO, CFO, CSO
D. Financial analyst, payroll clerk, HR manager

Answer: A

NEW QUESTION 6
- (Exam Topic 6)
A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP). In developing the business impact assessment (BIA), which of the following MOST closely relate to the data

backup and restoral?

A. Recovery Point Objective (RPO)
B. Mean Time to Delivery (MTD)
C. Recovery Time Objective (RTO)
D. Maximum Tolerable Downtime (MTD)

Answer: C

Explanation:
Reference:
https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#:~:text=The%2

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

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

Answer: C

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

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

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

Answer: D

NEW QUESTION 9
- (Exam Topic 6)
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 10
- (Exam Topic 6)
When reviewing a Solution as a Service (SaaS) provider’s security health and posture, which key document should you review?

A. SaaS provider’s website certifications and representations (certs and reps)
B. SOC-2 Report
C. Metasploit Audit Report
D. Statement from SaaS provider attesting their ability to secure your data

Answer: B

Explanation:
Reference: https://www.threatstack.com/blog/how-saas-companies-can-build-a-compliance-roadmap

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 13
- (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 18
- (Exam Topic 2)
Creating a secondary authentication process for network access would be an example of?

A. Nonlinearities in physical security performance metrics
B. Defense in depth cost enumerated costs
C. System hardening and patching requirements
D. Anti-virus for mobile devices

Answer: A

NEW QUESTION 21
- (Exam Topic 2)
Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

A. Application logs
B. File integrity monitoring
C. SNMP traps
D. Syslog

Answer: B

NEW QUESTION 22
- (Exam Topic 2)
When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

A. ISO 27001
B. PRINCE2
C. ISO 27004
D. ITILv3

Answer: C

NEW QUESTION 24
- (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 27
- (Exam Topic 2)
An organization has implemented a change management process for all changes to the IT production environment. This change management process follows best practices and is expected to help stabilize the availability and integrity of the organization's IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process:

A. Number of change orders rejected
B. Number and length of planned outages
C. Number of unplanned outages
D. Number of change orders processed

Answer: C

NEW QUESTION 32
- (Exam Topic 2)
Which of the following activities is the MAIN purpose of the risk assessment process?

A. Creating an inventory of information assets
B. Classifying and organizing information assets into meaningful groups
C. Assigning value to each information asset
D. Calculating the risks to which assets are exposed in their current setting

Answer: D

NEW QUESTION 34
- (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 35
- (Exam Topic 2)
When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

A. Transfer financial resources from other critical programs
B. Take the system off line until the budget is available
C. Deploy countermeasures and compensating controls until the budget is available
D. Schedule an emergency meeting and request the funding to fix the issue

Answer: C

NEW QUESTION 37
- (Exam Topic 2)
Creating a secondary authentication process for network access would be an example of?

A. An administrator with too much time on their hands.
B. Putting undue time commitment on the system administrator.
C. Supporting the concept of layered security
D. Network segmentation.

Answer: C

NEW QUESTION 39
- (Exam Topic 1)
What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

A. Determine appetite
B. Evaluate risk avoidance criteria
C. Perform a risk assessment
D. Mitigate risk

Answer: D

NEW QUESTION 41
- (Exam Topic 1)
Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

A. Awareness
B. Compliance
C. Governance
D. Management

Answer: C

NEW QUESTION 43
- (Exam Topic 1)
When choosing a risk mitigation method what is the MOST important factor?

A. Approval from the board of directors
B. Cost of the mitigation is less than the risk
C. Metrics of mitigation method success
D. Mitigation method complies with PCI regulations

Answer: B

NEW QUESTION 48
- (Exam Topic 1)
Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

A. Poses a strong technical background
B. Understand all regulations affecting the organization
C. Understand the business goals of the organization
D. Poses a strong auditing background

Answer: C

NEW QUESTION 49
- (Exam Topic 1)
Developing effective security controls is a balance between:

A. Risk Management and Operations
B. Corporate Culture and Job Expectations
C. Operations and Regulations
D. Technology and Vendor Management

Answer: A

NEW QUESTION 51
- (Exam Topic 1)
Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

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

Answer: D

NEW QUESTION 52
- (Exam Topic 1)
Risk appetite directly affects what part of a vulnerability management program?

A. Staff
B. Scope
C. Schedule
D. Scan tools

Answer: B

NEW QUESTION 53
- (Exam Topic 1)
Which of the following is a benefit of information security governance?

A. Questioning the trust in vendor relationships.
B. Increasing the risk of decisions based on incomplete management information.
C. Direct involvement of senior management in developing control processes
D. Reduction of the potential for civil and legal liability

Answer: D

NEW QUESTION 55
- (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 60

- (Exam Topic 1)
The Information Security Management program MUST protect:

A. all organizational assets
B. critical business processes and /or revenue streams
C. intellectual property released into the public domain
D. against distributed denial of service attacks

Answer: B

NEW QUESTION 63
- (Exam Topic 1)
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

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

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.
B. Establishing strategic alignment with bunsiness continuity requirements
C. Establishing incident response programs.
D. Identifying and implementing the best security solutions.

Answer: A

NEW QUESTION 69
- (Exam Topic 1)
Which of the following is the MOST important for a CISO to understand when identifying threats?

A. How vulnerabilities can potentially be exploited in systems that impact the organization
B. How the security operations team will behave to reported incidents
C. How the firewall and other security devices are configured to prevent attacks
D. How the incident management team prepares to handle an attack

Answer: A

NEW QUESTION 71
- (Exam Topic 1)
Which of the following most commonly falls within the scope of an information security governance steering committee?

A. Approving access to critical financial systems
B. Developing content for security awareness programs
C. Interviewing candidates for information security specialist positions
D. Vetting information security policies

Answer: D

NEW QUESTION 75
- (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 77
- (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 81
- (Exam Topic 1)
An organization information security policy serves to

A. establish budgetary input in order to meet compliance requirements
B. establish acceptable systems and user behavior
C. define security configurations for systems
D. define relationships with external law enforcement agencies

Answer: B

NEW QUESTION 82
- (Exam Topic 1)
Which of the following intellectual Property components is focused on maintaining brand recognition?

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

Answer: A

NEW QUESTION 87
- (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 91
- (Exam Topic 1)
When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

A. The asset owner
B. The asset manager
C. The data custodian
D. The project manager

Answer: A

NEW QUESTION 96
- (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 99
- (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 104
- (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 109
- (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 112
- (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 116
- (Exam Topic 1)
When briefing senior management on the creation of a governance process, the MOST important aspect should be:

A. information security metrics.
B. knowledge required to analyze each issue.
C. baseline against which metrics are evaluated.
D. linkage to business area objectives.

Answer: D

NEW QUESTION 120
- (Exam Topic 1)
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer: A

NEW QUESTION 122
- (Exam Topic 1)
Why is it vitally important that senior management endorse a security policy?

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.
D. So that they can be held legally accountable.

Answer: A

NEW QUESTION 127
- (Exam Topic 1)
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

A. The organization uses exclusively a quantitative process to measure risk
B. The organization uses exclusively a qualitative process to measure risk
C. The organization's risk tolerance is high
D. The organization's risk tolerance is lo

Answer: C

NEW QUESTION 129
- (Exam Topic 1)
The success of the Chief Information Security Officer is MOST dependent upon:

A. favorable audit findings
B. following the recommendations of consultants and contractors

C. development of relationships with organization executives
D. raising awareness of security issues with end users

Answer: C

NEW QUESTION 132
- (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 133
- (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 134
- (Exam Topic 1)
A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

A. Providing a risk program governance structure
B. Ensuring developers include risk control comments in code
C. Creating risk assessment templates based on specific threats
D. Allowing for the acceptance of risk for regulatory compliance requirements

Answer: A

NEW QUESTION 139
- (Exam Topic 1)
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization’s large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

A. Scan a representative sample of systems
B. Perform the scans only during off-business hours
C. Decrease the vulnerabilities within the scan tool settings
D. Filter the scan output so only pertinent data is analyzed

Answer: A

NEW QUESTION 140
- (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 141
- (Exam Topic 1)
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

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

Answer: B

NEW QUESTION 145
- (Exam Topic 1)
When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security

program?

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

Answer: C

NEW QUESTION 150
- (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 152
- (Exam Topic 6)
Which of the following statements below regarding Key Performance indicators (KPIs) are true?

A. Development of KPI's are most useful when done independently
B. They are a strictly quantitative measure of success
C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
D. They are a strictly qualitative measure of success

Answer: A

Explanation:
Reference: https://kpi.org/KPI-Basics/KPI-Development

NEW QUESTION 153
- (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 158
- (Exam Topic 6)
Who should be involved in the development of an internal campaign to address email phishing?

A. Business unit leaders, CIO, CEO
B. Business Unite Leaders, CISO, CIO and CEO
C. All employees
D. CFO, CEO, CIO

Answer: B

NEW QUESTION 160
- (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 165
- (Exam Topic 5)
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the “real workers.”
What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

A. Cite compliance with laws, statutes, and regulations – explaining the financial implications for the company for non-compliance
B. Understand the business and focus your efforts on enabling operations securely
C. Draw from your experience and recount stories of how other companies have been compromised
D. Cite corporate policy and insist on compliance with audit findings

Answer: B

NEW QUESTION 166
- (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 170
- (Exam Topic 5)
Which of the following is a common technology for visual monitoring?

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

Answer: A

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

NEW QUESTION 175
- (Exam Topic 5)
Which of the following best describes the sensors designed to project and detect a light beam across an area?

A. Smoke
B. Thermal
C. Air-aspirating
D. Photo electric

Answer: D

Explanation:
Reference: https://en.wikipedia.org/wiki/Photoelectric_sensor

NEW QUESTION 177
- (Exam Topic 5)
Using the Transport Layer Security (TLS) protocol enables a client in a network to be:

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

Answer: B

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

NEW QUESTION 178
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda. From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO’s approach to security?

A. Compliance centric agenda
B. IT security centric agenda
C. Lack of risk management process
D. Lack of sponsorship from executive management

Answer: B

NEW QUESTION 182
- (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 adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

A. Annually
B. Semi-annually
C. Quarterly
D. Never

Answer: D

NEW QUESTION 186
- (Exam Topic 5)
Which of the following is MOST useful when developing a business case for security initiatives?

A. Budget forecasts
B. Request for proposals
C. Cost/benefit analysis
D. Vendor management

Answer: C

NEW QUESTION 187
- (Exam Topic 5)
What are the three hierarchically related aspects of strategic planning and in which order should they be done?

A. 1) Information technology strategic planning, 2) Enterprise strategic planning, 3) Cybersecurity orinformation security strategic planning
B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3)Informationtechnology strategic planning
C. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning
D. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3)Information technology strategic planning

Answer: D

NEW QUESTION 189
- (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 191
- (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 196
- (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.
In what phase of the response will the team extract information from the affected systems without altering original data?

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

Answer: B

NEW QUESTION 197
- (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 198
- (Exam Topic 5)
When analyzing and forecasting a capital expense budget what are not included?

A. Network connectivity costs
B. New datacenter to operate from
C. Upgrade of mainframe
D. Purchase of new mobile devices to improve operations

Answer: A

NEW QUESTION 201
- (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 202
- (Exam Topic 5)
As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

A. Dual Control
B. Separation of Duties
C. Split Knowledge
D. Least Privilege

Answer: A

Explanation:
Reference: https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management

NEW QUESTION 204
- (Exam Topic 5)
Human resource planning for security professionals in your organization is a:

A. Simple and easy task because the threats are getting easier to find and correct.
B. Training requirement that is met through once every year user training.
C. Training requirement that is on-going and always changing.
D. Not needed because automation and anti-virus software has eliminated the threats.

Answer: C

NEW QUESTION 207
- (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 implemented remediation activities. Which of the following is the MOST logical next step?

A. Validate the effectiveness of applied controls
B. Validate security program resource requirements
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: A

NEW QUESTION 211
- (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 213
- (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 218
- (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 223
- (Exam Topic 5)
When analyzing and forecasting an operating expense budget what are not included?

A. Software and hardware license fees
B. Utilities and power costs
C. Network connectivity costs
D. New datacenter to operate from

Answer: D

NEW QUESTION 228
- (Exam Topic 5)
SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization’s needs.
The CISO is unsure of the information provided and orders a vendor proof of concept to validate the system’s scalability. This demonstrates which of the following?

A. An approach that allows for minimum budget impact if the solution is unsuitable
B. A methodology-based approach to ensure authentication mechanism functions
C. An approach providing minimum time impact to the implementation schedules
D. A risk-based approach to determine if the solution is suitable for investment

Answer: D

NEW QUESTION 230
- (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 231
- (Exam Topic 5)
A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

A. Poorly configured firewalls
B. Malware
C. Advanced Persistent Threat (APT)
D. An insider

Answer: D

NEW QUESTION 232
- (Exam Topic 5)
A newly-hired CISO needs to understand the organization's financial management standards for business units and operations. Which of the following would be the best source of this information?

A. The internal accounting department
B. The Chief Financial Officer (CFO)
C. The external financial audit service
D. The managers of the accounts payables and accounts receivables teams

Answer: D

NEW QUESTION 237
- (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 240
- (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 242
- (Exam Topic 5)
File Integrity Monitoring (FIM) is considered a

A. Network based security preventative control
B. Software segmentation control
C. Security detective control
D. User segmentation control

Answer: C

NEW QUESTION 243
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization. From an organizational perspective, which of the following is the LIKELY reason for this?

A. The CISO does not report directly to the CEO of the organization
B. The CISO reports to the IT organization
C. The CISO has not implemented a policy management framework
D. The CISO has not implemented a security awareness program

Answer: B

NEW QUESTION 247

- (Exam Topic 5)
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following
principles does this best demonstrate?

A. Effective use of existing technologies
B. Create a comprehensive security awareness program and provide success metrics to business units
C. Proper budget management
D. Leveraging existing implementations

Answer: B

NEW QUESTION 252
- (Exam Topic 5)
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the “real workers.”
Which group of people should be consulted when developing your security program?

A. Peers
B. End Users
C. Executive Management
D. All of the above

Answer: D

NEW QUESTION 255
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
Which of the following is the reason the CISO has not been able to advance the security agenda in this
organization?

A. Lack of identification of technology stake holders
B. Lack of business continuity process
C. Lack of influence with leaders outside IT
D. Lack of a security awareness program

Answer: C

NEW QUESTION 258
- (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 263
- (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 264
- (Exam Topic 5)
What is the primary reason for performing vendor management?

A. To understand the risk coverage that are being mitigated by the vendor
B. To establish a vendor selection process
C. To document the relationship between the company and the vendor
D. To define the partnership for long-term success

Answer: A

NEW QUESTION 265
- (Exam Topic 5)
Which of the following is an accurate description of a balance sheet?

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

Answer: C

NEW QUESTION 270
- (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 272
- (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 277
- (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 278
- (Exam Topic 5)
Which type of physical security control scan a person’s external features through a digital video camera before granting access to a restricted area?

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

Answer: C

NEW QUESTION 283
- (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 285

- (Exam Topic 5)
Which of the following is the MOST important reason for performing assessments of the security portfolio?

A. To assure that the portfolio is aligned to the needs of the broader organization
B. To create executive support of the portfolio
C. To discover new technologies and processes for implementation within the portfolio
D. To provide independent 3rd party reviews of security effectiveness

Answer: A

NEW QUESTION 286
- (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 288
- (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.
You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?

A. Get approval from the board of directors
B. Screen potential vendor solutions
C. Verify that the cost of mitigation is less than the risk
D. Create a risk metrics for all unmitigated risks

Answer: C

NEW QUESTION 289
- (Exam Topic 5)
The total cost of security controls should:

A. Be equal to the value of the information resource being protected
B. Be greater than the value of the information resource being protected
C. Be less than the value of the information resource being protected
D. Should not matter, as long as the information resource is protected

Answer: C

NEW QUESTION 294
- (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 296
- (Exam Topic 5)
As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

A. File Transfer Protocol (FTP)
B. Virtual Local Area Network (VLAN)
C. Simple Mail Transfer Protocol
D. Virtual Private Network (VPN)

Answer: D

Explanation:
Reference: https://searchnetworking.techtarget.com/definition/virtual-private-network

NEW QUESTION 301
- (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 306
- (Exam Topic 5)
A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website. This type of control is considered

A. Zero-day attack mitigation
B. Preventive detection control
C. Corrective security control
D. Dynamic blocking control

Answer: C

NEW QUESTION 308
- (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 311
- (Exam Topic 5)
A CISO has implemented a risk management capability within the security portfolio. Which of the following terms best describes this functionality?

A. Service
B. Program
C. Portfolio
D. Cost center

Answer: B

NEW QUESTION 313
- (Exam Topic 5)
Which technology can provide a computing environment without requiring a dedicated hardware backend?

A. Mainframe server
B. Virtual Desktop
C. Thin client
D. Virtual Local Area Network

Answer: B

NEW QUESTION 318
- (Exam Topic 4)
The process of identifying and classifying assets is typically included in the

A. Threat analysis process
B. Asset configuration management process
C. Business Impact Analysis
D. Disaster Recovery plan

Answer: B

NEW QUESTION 322
- (Exam Topic 4)
Which of the following is a symmetric encryption algorithm?

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

Answer: A

NEW QUESTION 324
- (Exam Topic 4)
Which of the following is the MAIN security concern for public cloud computing?

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

Answer: A

NEW QUESTION 329
- (Exam Topic 4)
One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys should be used to encrypt the message?

A. Your public key
B. The recipient's private key
C. The recipient's public key
D. Certificate authority key

Answer: C

NEW QUESTION 333
- (Exam Topic 4)
Physical security measures typically include which of the following components?

A. Physical, Technical, Operational
B. Technical, Strong Password, Operational
C. Operational, Biometric, Physical
D. Strong password, Biometric, Common Access Card

Answer: A

NEW QUESTION 337
- (Exam Topic 4)
Which of the following is a countermeasure to prevent unauthorized database access from web applications?

A. Session encryption
B. Removing all stored procedures
C. Input sanitization
D. Library control

Answer: C

NEW QUESTION 341
- (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 345
- (Exam Topic 4)
Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?

A. Comprehensive Log-Files from all servers and network devices affected during the attack
B. Fully trained network forensic experts to analyze all data right after the attack
C. Uninterrupted Chain of Custody
D. Expert forensics witness

Answer: C

NEW QUESTION 346
- (Exam Topic 4)
Which of the following statements about Encapsulating Security Payload (ESP) is true?

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

Answer: A

NEW QUESTION 349
- (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 353
- (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 357
- (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 360
- (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 363
- (Exam Topic 3)
Which of the following best summarizes the primary goal of a security program?

A. Provide security reporting to all levels of an organization
B. Create effective security awareness to employees
C. Manage risk within the organization
D. Assure regulatory compliance

Answer: C

NEW QUESTION 365
- (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 366
- (Exam Topic 3)
Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

A. Cost benefit
B. Risk appetite
C. Business continuity
D. Likelihood of impact

Answer: B

NEW QUESTION 368
- (Exam Topic 3)
Which of the following is considered a project versus a managed process?

A. monitoring external and internal environment during incident response
B. ongoing risk assessments of routine operations
C. continuous vulnerability assessment and vulnerability repair
D. installation of a new firewall system

Answer: D

NEW QUESTION 370
- (Exam Topic 3)
When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

A. Vendors uses their own laptop and logins with same admin credentials your security team uses
B. Vendor uses a company supplied laptop and logins using two factor authentication with same admin credentials your security team uses
C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials
D. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials

Answer: C

NEW QUESTION 375
- (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 376
- (Exam Topic 3)
Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

A. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
B. Create separate controls for the business units based on the types of business and functions they perform
C. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
D. Provide the business units with control mandates and schedules of audits for compliance validation

Answer: C

NEW QUESTION 379
- (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 381
- (Exam Topic 3)
Which of the following is considered one of the most frequent failures in project management?

A. Overly restrictive management
B. Excessive personnel on project

C. Failure to meet project deadlines
D. Insufficient resources

Answer: C

NEW QUESTION 382
- (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 385
- (Exam Topic 3)
A stakeholder is a person or group:

A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
B. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
C. That has budget authority.
D. That will ultimately use the system.

Answer: A

NEW QUESTION 389
- (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 390
- (Exam Topic 3)
Which of the following are not stakeholders of IT security projects?

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

Answer: B

NEW QUESTION 395
- (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 396
- (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 398
- (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 401
- (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 405
- (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 408
- (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 412
- (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 413
- (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 417
- (Exam Topic 3)
You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

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

Answer: B

NEW QUESTION 422
- (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 427
- (Exam Topic 3)
Which business stakeholder is accountable for the integrity of a new information system?

A. CISO
B. Compliance Officer
C. Project manager
D. Board of directors

Answer: A

NEW QUESTION 432
- (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 436
- (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 440
- (Exam Topic 3)
Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed. What can be done to ensure that security is addressed cost effectively?

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

Answer: D

NEW QUESTION 445
- (Exam Topic 3)
A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability. What do you do?

A. tell him to shut down the server
B. tell him to call the police
C. tell him to invoke the incident response process
D. tell him to analyze the problem, preserve the evidence and provide a full analysis and report

Answer: C

NEW QUESTION 448
- (Exam Topic 3)
When managing the critical path of an IT security project, which of the following is MOST important?

A. Knowing who all the stakeholders are.
B. Knowing the people on the data center team.
C. Knowing the threats to the organization.
D. Knowing the milestones and timelines of deliverables.

Answer: D

NEW QUESTION 451
- (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 456
- (Exam Topic 2)
The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

A. assign the responsibility to the information security team.
B. assign the responsibility to the team responsible for the management of the controls.
C. create operational reports on the effectiveness of the controls.
D. perform an independent audit of the security controls.

Answer: D

NEW QUESTION 461
- (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 462
- (Exam Topic 2)
Dataflow diagrams are used by IT auditors to:

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

Answer: C

NEW QUESTION 466
- (Exam Topic 2)
Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

A. Single loss expectancy multiplied by the annual rate of occurrence
B. Total loss expectancy multiplied by the total loss frequency
C. Value of the asset multiplied by the loss expectancy
D. Replacement cost multiplied by the single loss expectancy

Answer: A

NEW QUESTION 469
- (Exam Topic 2)
Which of the following are primary concerns for management with regard to assessing internal control objectives?

A. Confidentiality, Availability, Integrity
B. Compliance, Effectiveness, Efficiency
C. Communication, Reliability, Cost
D. Confidentiality, Compliance, Cost

Answer: B

NEW QUESTION 474
- (Exam Topic 2)

At which point should the identity access management team be notified of the termination of an employee?

A. At the end of the day once the employee is off site
B. During the monthly review cycle
C. Immediately so the employee account(s) can be disabled
D. Before an audit

Answer: C

NEW QUESTION 477
- (Exam Topic 2)
Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

A. Servers, routers, switches, modem
B. Firewall, exchange, web server, intrusion detection system (IDS)
C. Firewall, anti-virus console, IDS, syslog
D. IDS, syslog, router, switches

Answer: C

NEW QUESTION 481
- (Exam Topic 2)
The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

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

Answer: D

NEW QUESTION 483
- (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 487
- (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 488
- (Exam Topic 2)
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

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

Answer: B

NEW QUESTION 490
- (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 495
- (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 499
- (Exam Topic 2)
Which of the following is the MOST important goal of risk management?

A. Identifying the risk
B. Finding economic balance between the impact of the risk and the cost of the control
C. Identifying the victim of any potential exploits.
D. Assessing the impact of potential threats

Answer: B

NEW QUESTION 504
- (Exam Topic 2)
A missing/ineffective security control is identified. Which of the following should be the NEXT step?

A. Perform an audit to measure the control formally
B. Escalate the issue to the IT organization
C. Perform a risk assessment to measure risk
D. Establish Key Risk Indicators

Answer: C

NEW QUESTION 506
- (Exam Topic 2)
You have implemented the new controls. What is the next step?

A. Document the process for the stakeholders
B. Monitor the effectiveness of the controls
C. Update the audit findings report
D. Perform a risk assessment

Answer: B

NEW QUESTION 510
- (Exam Topic 2)
When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

A. Threat Level, Risk of Compromise, and Consequences of Compromise
B. Risk Avoidance, Threat Level, and Consequences of Compromise
C. Risk Transfer, Reputational Impact, and Consequences of Compromise
D. Reputational Impact, Financial Impact, and Risk of Compromise

Answer: A

NEW QUESTION 515
- (Exam Topic 2)
You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

A. Validate that security awareness program content includes information about the potential vulnerability
B. Conduct a thorough risk assessment against the current implementation to determine system functions
C. Determine program ownership to implement compensating controls
D. Send a report to executive peers and business unit owners detailing your suspicions

Answer: B

NEW QUESTION 517
- (Exam Topic 2)
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

A. Lack of notification to the public of disclosure of confidential information.
B. Lack of periodic examination of access rights
C. Failure to notify police of an attempted intrusion
D. Lack of reporting of a successful denial of service attack on the network.

Answer: A

NEW QUESTION 518

.....

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/