Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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

NEW QUESTION 1
- (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 2
- (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 3
- (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 4
- (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 5
- (Exam Topic 6)
From the CISO's perspective in looking at financial statements, the statement of retained earnings of an organization:

A. Has a direct correlation with the CISO's budget
B. Represents, in part, the savings generated by the proper acquisition and implementation of security controls
C. Represents the sum of all capital expenditures
D. Represents the percentage of earnings that could in part be used to finance future security controls

Answer: D

Explanation:
Reference: https://www.investopedia.com/terms/s/statement-of-retained-earnings.asp

NEW QUESTION 6
- (Exam Topic 6)
When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

A. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
B. Contracting rules typically require you to have conversations with two or more groups

C. Discussing decisions with a very large group of people always provides a better outcome
D. It helps to avoid regulatory or internal compliance issues

Answer: D

Explanation:
Reference:
https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf

NEW QUESTION 7
- (Exam Topic 6)
The main purpose of the SOC is:

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

Answer: C

Explanation:
Reference: https://www.eccouncil.org/what-is-soc/

NEW QUESTION 8
- (Exam Topic 6)
What key technology can mitigate ransomware threats?

A. Use immutable data storage
B. Phishing exercises
C. Application of multiple end point anti-malware solutions
D. Blocking use of wireless networks

Answer: A

Explanation:
Reference:
https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks

NEW QUESTION 9
- (Exam Topic 6)
The Board of Directors of a publicly-traded company is concerned about the security implications of a strategic project that will migrate 50% of the organization's information technology assets to the cloud. They have requested a briefing on the project plan and a progress report of the security stream of the project. As the CISO, you have been tasked with preparing the report for the Chief Executive Officer to present.
Using the Earned Value Management (EVM), what does a Cost Variance (CV) of -1,200 mean?

A. The project is over budget
B. The project budget has reserves
C. The project cost is in alignment with the budget
D. The project is under budget

Answer: A

Explanation:
Reference:
https://www.pmi.org/learning/library/earned-value-management-systems-analysis-8026#:~:text=The%20cost%2

NEW QUESTION 10
- (Exam Topic 6)
A bastion host should be placed:

A. Inside the DMZ
B. In-line with the data center firewall
C. Beyond the outer perimeter firewall
D. As the gatekeeper to the organization's honeynet

Answer: C

Explanation:
Reference: https://www.skillset.com/questions/a-bastion-host-is-which-of-the-following

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 12
- (Exam Topic 6)
Which of the following is the MOST effective method to counter phishing attacks?

A. User awareness and training
B. Host based Intrusion Detection System (IPS)
C. Acceptable use guide signed by all system users
D. Antispam solution

Answer: A

Explanation:
Reference: https://aware.eccouncil.org/4-best-ways-to-stop-phishing-with-security-awareness.html

NEW QUESTION 16
- (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 20
- (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 23
- (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)
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

A. Use within an organization to formulate security requirements and objectives
B. Implementation of business-enabling information security
C. Use within an organization to ensure compliance with laws and regulations
D. To enable organizations that adopt it to obtain certifications

Answer: B

NEW QUESTION 26
- (Exam Topic 2)
The effectiveness of an audit is measured by?

A. The number of actionable items in the recommendations
B. How it exposes the risk tolerance of the company
C. How the recommendations directly support the goals of the company
D. The number of security controls the company has in use

Answer: C

NEW QUESTION 30
- (Exam Topic 2)
An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

A. Management Control
B. Technical Control
C. Training Control
D. Operational Control

Answer: D

NEW QUESTION 31
- (Exam Topic 2)
A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

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

Answer: C

NEW QUESTION 36
- (Exam Topic 2)
Which of the following is a fundamental component of an audit record?

A. Date and time of the event
B. Failure of the event
C. Originating IP-Address
D. Authentication type

Answer: A

NEW QUESTION 41
- (Exam Topic 2)
Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

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

Answer: B

NEW QUESTION 45
- (Exam Topic 2)
To have accurate and effective information security policies how often should the CISO review the organization policies?

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

Answer: D

NEW QUESTION 46
- (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 49
- (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 52
- (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 57
- (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 60
- (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 64
- (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 65
- (Exam Topic 1)
When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

A. Escalation
B. Recovery
C. Eradication
D. Containment

Answer: D

NEW QUESTION 67
- (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 70
- (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 73
- (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 74
- (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 76
- (Exam Topic 1)
The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for

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

Answer: A

NEW QUESTION 79
- (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 80
- (Exam Topic 1)
You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

A. Chief Information Security Officer
B. Chief Executive Officer
C. Chief Information Officer
D. Chief Legal Counsel

Answer: B

NEW QUESTION 85
- (Exam Topic 1)
What is the first thing that needs to be completed in order to create a security program for your organization?

A. Risk assessment
B. Security program budget
C. Business continuity plan
D. Compliance and regulatory analysis

Answer: A

NEW QUESTION 88
- (Exam Topic 1)
Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

A. Need to comply with breach disclosure laws
B. Need to transfer the risk associated with hosting PII data
C. Need to better understand the risk associated with using PII data
D. Fiduciary responsibility to safeguard credit card information

Answer: C

NEW QUESTION 90
- (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 94
- (Exam Topic 1)
When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

A. When there is a need to develop a more unified incident response capability.
B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
C. When there is a variety of technologies deployed in the infrastructure.
D. When it results in an overall lower cost of operating the security program.

Answer: B

NEW QUESTION 98
- (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 103
- (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 105
- (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 108
- (Exam Topic 1)
You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

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

Answer:

C

NEW QUESTION 109
- (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 112
- (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 117
- (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 118
- (Exam Topic 1)
The FIRST step in establishing a security governance program is to?

A. Conduct a risk assessment.
B. Obtain senior level sponsorship.
C. Conduct a workshop for all end users.
D. Prepare a security budget.

Answer: B

NEW QUESTION 121
- (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 125
- (Exam Topic 1)
The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

A. Due Protection
B. Due Care
C. Due Compromise
D. Due process

Answer: B

NEW QUESTION 126
- (Exam Topic 1)
According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

A. Identify threats, risks, impacts and vulnerabilities
B. Decide how to manage risk
C. Define the budget of the Information Security Management System

D. Define Information Security Policy

Answer: D

NEW QUESTION 130
- (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 132
- (Exam Topic 1)
If your organization operates under a model of "assumption of breach", you should:

A. Protect all information resource assets equally
B. Establish active firewall monitoring protocols
C. Purchase insurance for your compliance liability
D. Focus your security efforts on high value assets

Answer: C

NEW QUESTION 136
- (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 138
- (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 142
- (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 144
- (Exam Topic 1)
Payment Card Industry (PCI) compliance requirements are based on what criteria?

A. The types of cardholder data retained
B. The duration card holder data is retained
C. The size of the organization processing credit card data
D. The number of transactions performed per year by an organization

Answer: D

NEW QUESTION 145
- (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 150
- (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 151
- (Exam Topic 1)
Which of the following are the MOST important factors for proactively determining system vulnerabilities?

A. Subscribe to vendor mailing list to get notification of system vulnerabilities
B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
D. Conduct security testing, vulnerability scanning, and penetration testing

Answer: D

NEW QUESTION 153
- (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 156
- (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 157
- (Exam Topic 1)
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

A. Audit and Legal
B. Budget and Compliance
C. Human Resources and Budget
D. Legal and Human Resources

Answer: A

NEW QUESTION 158
- (Exam Topic 6)
What are the common data hiding techniques used by criminals?

A. Unallocated space and masking
B. Website defacement and log manipulation
C. Disabled Logging and admin elevation
D. Encryption, Steganography, and Changing Metadata/Timestamps

Answer: D

Explanation:
Reference: https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/

NEW QUESTION 160
- (Exam Topic 6)
You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans.
Which control is MOST important to protect AI products?

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

Answer: D

NEW QUESTION 163
- (Exam Topic 6)
You have been hired as the Information System Security Officer (ISSO) for a US federal government agency. Your role is to ensure the security posture of the system is maintained. One of your tasks is to develop and maintain the system security plan (SSP) and supporting documentation.
Which of the following is NOT documented in the SSP?

A. The controls in place to secure the system
B. Name of the connected system
C. The results of a third-party audits and recommendations
D. Type of information used in the system

Answer: C

Explanation:
Reference:
https://www.govinfo.gov/content/pkg/GOVPUB-C13-63e84ab7af43b36228f10e4f0b5f8c38/pdf/GOVPUB-C13- (65)

NEW QUESTION 164
- (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 168
- (Exam Topic 6)
With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

A. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
B. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program
C. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

Answer: C

Explanation:
Reference: https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf (9)

NEW QUESTION 171
- (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 176
- (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 180
- (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 182
- (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 186
- (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 187
- (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 192
- (Exam Topic 5)
Which of the following is true regarding expenditures?

A. Capital expenditures are never taxable
B. Operating expenditures are for acquiring assets, capital expenditures are for support costs of that asset
C. Capital expenditures are used to define depreciation tables of intangible assets
D. Capital expenditures are for acquiring assets, whereas operating expenditures are for support costs of that asset

Answer: D

NEW QUESTION 194
- (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 198
- (Exam Topic 5)
Which of the following information would MOST likely be reported at the board-level within an organization?

A. System scanning trends and results as they pertain to insider and external threat sources
B. The capabilities of a security program in terms of staffing support
C. Significant risks and security incidents that have been discovered since the last assembly of the membership
D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

Answer: C

NEW QUESTION 201
- (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 202
- (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 205
- (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 208
- (Exam Topic 5)
Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

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

Answer: A

NEW QUESTION 212
- (Exam Topic 5)
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline

of a security policy and recommend an industry/sector neutral information security control framework for implementation.
Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

A. National Institute of Standards and Technology (NIST) Special Publication 800-53
B. Payment Card Industry Digital Security Standard (PCI DSS)
C. International Organization for Standardization – ISO 27001/2
D. British Standard 7799 (BS7799)

Answer: C

NEW QUESTION 217
- (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 222
- (Exam Topic 5)
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN.
What type of control is being implemented by supervisors and data owners?

A. Management
B. Operational
C. Technical
D. Administrative

Answer: B

NEW QUESTION 226
- (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 229
- (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 230
- (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 233
- (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 238
- (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 239
- (Exam Topic 5)
John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can John do in this instance?

A. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
B. Review the Request for Proposal (RFP) for guidance.
C. Withhold the vendor's payments until the issue is resolved.
D. Refer to the contract agreement for direction.

Answer: D

NEW QUESTION 244
- (Exam Topic 5)
During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

A. The budget is in a temporary state of imbalance
B. The budget is operating at a deficit
C. She can realign the budget through moderate capital expense (CAPEX) allocation
D. She has a surplus of operational expenses (OPEX)

Answer: A

NEW QUESTION 245
- (Exam Topic 5)
Which of the following best describes a portfolio?

A. The portfolio is used to manage and track individual projects
B. The portfolio is used to manage incidents and events
C. A portfolio typically consists of several programs
D. A portfolio delivers one specific service or program to the business

Answer: C

NEW QUESTION 250
- (Exam Topic 5)
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.
Your Corporate Information Security Policy should include which of the following?

A. Information security theory
B. Roles and responsibilities
C. Incident response contacts
D. Desktop configuration standards

Answer: B

NEW QUESTION 252
- (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 257
- (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.
What is the MOST logical course of action the CISO should take?

A. Review the original solution set to determine if another system would fit the organization's risk appetite and budgetregulatory compliance requirements
B. Continue with the implementation and submit change requests to the vendor in order to ensure required functionality will be provided when needed
C. Continue with the project until the scalability issue is validated by others, such as an auditor or third party assessor
D. Cancel the project if the business need was based on internal requirements versus regulatory compliance requirements

Answer: A

NEW QUESTION 259
- (Exam Topic 5)
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
The organization has already been subject to a significant amount of credit card fraud. Which of the following is the MOST likely reason for this fraud?

A. Lack of compliance to the Payment Card Industry (PCI) standards
B. Ineffective security awareness program
C. Security practices not in alignment with ISO 27000 frameworks
D. Lack of technical controls when dealing with credit card data

Answer: A

NEW QUESTION 263
- (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 265
- (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 266
- (Exam Topic 5)
At what level of governance are individual projects monitored and managed?

A. Program
B. Milestone
C. Enterprise
D. Portfolio

Answer: D

NEW QUESTION 271
- (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 273
- (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 277
- (Exam Topic 5)
Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

A. The Net Present Value (NPV) of the project is positive
B. The NPV of the project is negative
C. The Return on Investment (ROI) is larger than 10 months
D. The ROI is lower than 10 months

Answer: B

NEW QUESTION 281
- (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 284
- (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 289
- (Exam Topic 5)
Acceptable levels of information security risk tolerance in an organization should be determined by?

A. Corporate legal counsel
B. CISO with reference to the company goals
C. CEO and board of director
D. Corporate compliance committee

Answer: C

NEW QUESTION 291
- (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 295
- (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 298
- (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 299
- (Exam Topic 5)
When creating contractual agreements and procurement processes why should security requirements be included?

A. To make sure they are added on after the process is completed
B. To make sure the costs of security is included and understood
C. To make sure the security process aligns with the vendor's security process
D. To make sure the patching process is included with the costs

Answer: B

NEW QUESTION 301
- (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.
Which of the following is the FIRST action the CISO will perform after receiving the audit report?

A. Inform peer executives of the audit results
B. Validate gaps and accept or dispute the audit findings
C. Create remediation plans to address program gaps
D. Determine if security policies and procedures are adequate

Answer: B

NEW QUESTION 306
- (Exam Topic 5)
If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the BEST control to safeguard data integrity?

A. Backup to tape
B. Maintain separate VM backups
C. Backup to a remote location
D. Increase VM replication frequency

Answer: B

Explanation:
Reference:
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/is-audit-basics-backup-andrecovery

NEW QUESTION 310
- (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 313
- (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 314
- (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 317
- (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 319
- (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 322
- (Exam Topic 5)
You are just hired as the new CISO and are being briefed on all the Information Security projects that your
section has on going. You discover that most projects are behind schedule and over budget.
Using the best business practices for project management you determine that the project correct aligns with the company goals. What needs to be verified FIRST?

A. Scope of the project
B. Training of the personnel on the project
C. Timeline of the project milestones
D. Vendor for the project

Answer: A

NEW QUESTION 324
- (Exam Topic 5)
What is the difference between encryption and tokenization?

A. Tokenization combined with hashing is always better than encryption
B. Encryption can be mathematically reversed to provide the original information
C. The token contains the all original information
D. Tokenization can be mathematically reversed to provide the original information

Answer: B

Explanation:
Reference:
http://library.ahima.org/doc?oid=104090#.X_dwWolR3eQ

NEW QUESTION 328
- (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 331
- (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 334
- (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 339
- (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. Once supervisors and data owners have approved requests, information system administrators will implement

A. Technical control(s)
B. Management control(s)
C. Policy control(s)
D. Operational control(s)

Answer: A

NEW QUESTION 340
- (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 343
- (Exam Topic 5)
Which of the following would negatively impact a log analysis of a multinational organization?

A. Centralized log management
B. Encrypted log files in transit

C. Each node set to local time
D. Log aggregation agent each node

Answer: D

NEW QUESTION 345
- (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 349
- (Exam Topic 4)
What type of attack requires the least amount of technical equipment and has the highest success rate?

A. War driving
B. Operating system attacks
C. Social engineering
D. Shrink wrap attack

Answer: C

NEW QUESTION 350
- (Exam Topic 4)
The process for identifying, collecting, and producing digital information in support of legal proceedings is called

A. chain of custody.
B. electronic discovery.
C. evidence tampering.
D. electronic review.

Answer: B

NEW QUESTION 355
- (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 358
- (Exam Topic 4)
An anonymity network is a series of?

A. Covert government networks
B. War driving maps
C. Government networks in Tora
D. Virtual network tunnels

Answer: D

NEW QUESTION 362
- (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 366
- (Exam Topic 4)

Which wireless encryption technology makes use of temporal keys?

A. Wireless Application Protocol (WAP)
B. Wifi Protected Access version 2 (WPA2)
C. Wireless Equivalence Protocol (WEP)
D. Extensible Authentication Protocol (EAP)

Answer: B

NEW QUESTION 367
- (Exam Topic 3)
To get an Information Security project back on schedule, which of the following will provide the MOST help?

A. Upper management support
B. More frequent project milestone meetings
C. Stakeholder support
D. Extend work hours

Answer: A

NEW QUESTION 372
- (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 376
- (Exam Topic 4)
Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the incident handling process will utilize the signature to resolve this incident?

A. Containment
B. Recovery
C. Identification
D. Eradication

Answer: D

NEW QUESTION 380
- (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 382
- (Exam Topic 3)
Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

A. Upper management support
B. More frequent project milestone meetings
C. More training of staff members
D. Involve internal audit

Answer: A

NEW QUESTION 384
- (Exam Topic 3)
This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

A. Scope creep
B. Deadline extension
C. Scope modification
D. Deliverable expansion

Answer: A

NEW QUESTION 387
- (Exam Topic 3)
The organization does not have the time to remediate the vulnerability; however it is critical to release the application. Which of the following needs to be further evaluated to help mitigate the risks?

A. Provide developer security training
B. Deploy Intrusion Detection Systems
C. Provide security testing tools
D. Implement Compensating Controls

Answer: D

NEW QUESTION 390
- (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 391
- (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 392
- (Exam Topic 3)
When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

A. Type of data contained in the process/system
B. Type of connection/protocol used to transfer the data
C. Type of encryption required for the data once it is at rest
D. Type of computer the data is processed on

Answer: A

NEW QUESTION 394
- (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 398
- (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 401
- (Exam Topic 3)
Your company has a "no right to privacy" notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this

condition. A peer group member and friend comes to you and requests access to one of her employee's email account. What should you do? (choose the BEST answer):

A. Grant her access, the employee has been adequately warned through the AUP.
B. Assist her with the request, but only after her supervisor signs off on the action.
C. Reset the employee's password and give it to the supervisor.
D. Deny the request citing national privacy laws.

Answer: B

NEW QUESTION 405
- (Exam Topic 3)
A recommended method to document the respective roles of groups and individuals for a given process is to:

A. Develop a detailed internal organization chart
B. Develop a telephone call tree for emergency response
C. Develop an isolinear response matrix with cost benefit analysis projections
D. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart

Answer: D

NEW QUESTION 410
- (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 415
- (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 418
- (Exam Topic 3)
Which of the following methodologies references the recommended industry standard that Information security project managers should follow?

A. The Security Systems Development Life Cycle
B. The Security Project And Management Methodology
C. Project Management System Methodology
D. Project Management Body of Knowledge

Answer: D

NEW QUESTION 421
- (Exam Topic 3)
A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:

A. Change management
B. Business continuity planning
C. Security Incident Response
D. Thought leadership

Answer: C

NEW QUESTION 422
- (Exam Topic 3)
In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?

A. Vmware, router, switch, firewall, syslog, vulnerability management system (VMS)
B. Intrusion Detection System (IDS), firewall, switch, syslog
C. Security Incident Event Management (SIEM), IDS, router, syslog
D. SIEM, IDS, firewall, VMS

Answer: D

NEW QUESTION 427
- (Exam Topic 3)
A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims. Which of the following vendor provided documents is BEST to make your decision:

A. Vendor's client list of reputable organizations currently using their solution
B. Vendor provided attestation of the detailed security controls from a reputable accounting firm
C. Vendor provided reference from an existing reputable client detailing their implementation
D. Vendor provided internal risk assessment and security control documentation

Answer: B

NEW QUESTION 432
- (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 435
- (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 440
- (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 441
- (Exam Topic 3)
Which of the following is critical in creating a security program aligned with an organization's goals?

A. Ensure security budgets enable technical acquisition and resource allocation based on internal compliance requirements
B. Develop a culture in which users, managers and IT professionals all make good decisions about information risk
C. Provide clear communication of security program support requirements and audit schedules
D. Create security awareness programs that include clear definition of security program goals and charters

Answer: B

NEW QUESTION 442
- (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 443
- (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 444
- (Exam Topic 3)
An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents. Which of the following would be considered a MAJOR constraint for the project?

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

Answer: C

NEW QUESTION 446
- (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 451
- (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 455
- (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 458
- (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 462
- (Exam Topic 3)
When entering into a third party vendor agreement for security services, at what point in the process is it BEST to understand and validate the security posture and compliance level of the vendor?

A. At the time the security services are being performed and the vendor needs access to the network
B. Once the agreement has been signed and the security vendor states that they will need access to the network
C. Once the vendor is on premise and before they perform security services
D. Prior to signing the agreement and before any security services are being performed

Answer: D

NEW QUESTION 467
- (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 472
- (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 476
- (Exam Topic 2)
An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application. What should be the NEXT step?

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

Answer: C

NEW QUESTION 477
- (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 480
- (Exam Topic 2)
Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

A. Detective Controls
B. Proactive Controls
C. Preemptive Controls
D. Organizational Controls

Answer: D

NEW QUESTION 485
- (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 487
- (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 490
- (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 491
- (Exam Topic 2)
Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

A. To give information security management recommendations to those who are responsible for initiating, implementing, or maintaining security in their organization.
B. To provide a common basis for developing organizational security standards
C. To provide effective security management practice and to provide confidence in inter-organizational dealings
D. To established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization

Answer: D

NEW QUESTION 495
- (Exam Topic 2)
The risk found after a control has been fully implemented is called:

A. Residual Risk
B. Total Risk
C. Post implementation risk
D. Transferred risk

Answer: A

NEW QUESTION 496
- (Exam Topic 2)
Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

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

Answer: A

NEW QUESTION 500
- (Exam Topic 2)
An information security department is required to remediate system vulnerabilities when they are discovered.
Please select the three primary remediation methods that can be used on an affected system.

A. Install software patch, Operate system, Maintain system
B. Discover software, Remove affected software, Apply software patch
C. Install software patch, configuration adjustment, Software Removal
D. Software removal, install software patch, maintain system

Answer: C

NEW QUESTION 503
- (Exam Topic 2)
As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

A. Executive summary
B. Penetration test agreement
C. Names and phone numbers of those who conducted the audit
D. Business charter

Answer: A

NEW QUESTION 506
- (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 509
- (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 513
- (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 514
- (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 517
- (Exam Topic 2)
Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

A. Plan-Check-Do-Act
B. Plan-Do-Check-Act
C. Plan-Select-Implement-Evaluate
D. SCORE (Security Consensus Operational Readiness Evaluation)

Answer: B

NEW QUESTION 519
- (Exam Topic 2)
Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

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

Answer: A

NEW QUESTION 520
- (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 521
- (Exam Topic 2)
Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

A. Incident response plan
B. Business Continuity plan
C. Disaster recovery plan
D. Damage control plan

Answer: C

NEW QUESTION 525
- (Exam Topic 2)
The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is

A. Penetration testers
B. External Audit
C. Internal Audit
D. Forensic experts

Answer: B

NEW QUESTION 530
- (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 534
- (Exam Topic 2)
The patching and monitoring of systems on a consistent schedule is required by?

A. Local privacy laws
B. Industry best practices
C. Risk Management frameworks
D. Audit best practices

Answer: C

NEW QUESTION 539
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

712-50 Practice Exam Features:

* 712-50 Questions and Answers Updated Frequently

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

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

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