EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 6)
Devising controls for information security is a balance between?

A. Governance and compliance
B. Auditing and security
C. Budget and risk tolerance
D. Threats and vulnerabilities

Answer: C

Explanation:
Reference: https://www.cybok.org/media/downloads/cybok_version_1.0.pdf

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

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

Answer: A

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

NEW QUESTION 7
- (Exam Topic 6)
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 8
- (Exam Topic 6)
Who is responsible for verifying that audit directives are implemented?

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

Answer: B

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

NEW QUESTION 9
- (Exam Topic 6)
In defining a strategic security plan for an organization, what should a CISO first analyze?

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

Answer: D

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

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

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

Answer: C

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

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

Answer: A

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

NEW QUESTION 13
- (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 17
- (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 you develop your audit remediation plan what is the MOST important criteria?

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

Answer: C

NEW QUESTION 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 28
- (Exam Topic 2)
When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

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

Answer: A

NEW QUESTION 29
- (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 32
- (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 34
- (Exam Topic 2)
Which of the following are necessary to formulate responses to external audit findings?

A. Internal Audit, Management, and Technical Staff
B. Internal Audit, Budget Authority, Management
C. Technical Staff, Budget Authority, Management
D. Technical Staff, Internal Audit, Budget Authority

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 42
- (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 46
- (Exam Topic 1)
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

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

Answer: B

NEW QUESTION 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 51
- (Exam Topic 1)
When managing the security architecture for your company you must consider:

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

Answer: D

NEW QUESTION 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 56
- (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 57
- (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 59
- (Exam Topic 1)
One of the MAIN goals of a Business Continuity Plan is to

A. Ensure all infrastructure and applications are available in the event of a disaster
B. Allow all technical first-responders to understand their roles in the event of a disaster
C. Provide step by step plans to recover business processes in the event of a disaster
D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer: C

NEW QUESTION 63
- (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 71
- (Exam Topic 1)
What is the main purpose of the Incident Response Team?

A. Ensure efficient recovery and reinstate repaired systems
B. Create effective policies detailing program activities
C. Communicate details of information security incidents
D. Provide current employee awareness programs

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 77
- (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 78
- (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 79
- (Exam Topic 1)
A method to transfer risk is to:

A. Implement redundancy
B. move operations to another region
C. purchase breach insurance
D. Alignment with business operations

Answer: C

NEW QUESTION 80
- (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 83
- (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 86
- (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 88

- (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 91
- (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 96
- (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 97
- (Exam Topic 1)
What is the BEST way to achieve on-going compliance monitoring in an organization?

A. Only check compliance right before the auditors are scheduled to arrive onsite.
B. Outsource compliance to a 3rd party vendor and let them manage the program.
C. Have Compliance and Information Security partner to correct issues as they arise.
D. Have Compliance direct Information Security to fix issues after the auditors report.

Answer: C

NEW QUESTION 102
- (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 105
- (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 108
- (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 110
- (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 115
- (Exam Topic 1)
When dealing with a risk management process, asset classification is important because it will impact the overall:

A. Threat identification
B. Risk monitoring
C. Risk treatment
D. Risk tolerance

Answer: C

NEW QUESTION 119
- (Exam Topic 1)
Which of the following is a critical operational component of an Incident Response Program (IRP)?

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

Answer: C

NEW QUESTION 123
- (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 127
- (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 128
- (Exam Topic 1)
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

A. Lack of a formal security awareness program
B. Lack of a formal security policy governance process
C. Lack of formal definition of roles and responsibilities
D. Lack of a formal risk management policy

Answer: B

NEW QUESTION 132
- (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 134
- (Exam Topic 1)
What is the MAIN reason for conflicts between Information Technology and Information Security programs?

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

Answer: D

NEW QUESTION 138
- (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 142
- (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 145
- (Exam Topic 1)
An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System. Which of the following international standards can BEST assist this organization?

A. International Organization for Standardizations – 27004 (ISO-27004)
B. Payment Card Industry Data Security Standards (PCI-DSS)
C. Control Objectives for Information Technology (COBIT)
D. International Organization for Standardizations – 27005 (ISO-27005)

Answer: A

NEW QUESTION 148
- (Exam Topic 1)
Regulatory requirements typically force organizations to implement

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

Answer: A

NEW QUESTION 152
- (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 157
- (Exam Topic 1)
Ensuring that the actions of a set of people, applications and systems follow the organization’s rules is BEST described as:

A. Risk management
B. Security management

C. Mitigation management
D. Compliance management

Answer: D

NEW QUESTION 162
- (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 163
- (Exam Topic 1)
When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

A. An independent Governance, Risk and Compliance organization
B. Alignment of security goals with business goals
C. Compliance with local privacy regulations
D. Support from Legal and HR teams

Answer: B

NEW QUESTION 168
- (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 172
- (Exam Topic 1)
What is the relationship between information protection and regulatory compliance?

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

Answer: C

NEW QUESTION 177
- (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 182
- (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 184
- (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 188
- (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 192
- (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 194
- (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 197
- (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 198
- (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 199
- (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 203
- (Exam Topic 5)
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
When multiple regulations or standards apply to your industry you should set controls to meet the:

A. Easiest regulation or standard to implement
B. Stricter regulation or standard
C. Most complex standard to implement
D. Recommendations of your Legal Staff

Answer: C

NEW QUESTION 206
- (Exam Topic 5)
What are the three stages of an identity and access management system?

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

Answer: A

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

NEW QUESTION 211
- (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 213
- (Exam Topic 5)
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company's building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

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

Answer: B

NEW QUESTION 216
- (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 221
- (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 222
- (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 225
- (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 229
- (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 231
- (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 234
- (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 235
- (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 237
- (Exam Topic 5)
The newly appointed CISO of an organization is reviewing the IT security strategic plan. Which of the following is the MOST important component of the strategic plan?

A. There is integration between IT security and business staffing.
B. There is a clear definition of the IT security mission and vision.
C. There is an auditing methodology in place.
D. The plan requires return on investment for all security projects.

Answer: B

NEW QUESTION 239
- (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 243
- (Exam Topic 5)
The formal certification and accreditation process has four primary steps, what are they?

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

Answer: A

NEW QUESTION 246
- (Exam Topic 5)
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.
Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

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

Answer: A

NEW QUESTION 248
- (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 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 256
- (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 261
- (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 262
- (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 264
- (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 266
- (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 268
- (Exam Topic 5)
Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:

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

Answer: B

NEW QUESTION 270
- (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 272
- (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 276
- (Exam Topic 5)
When project costs continually increase throughout implementation due to large or rapid changes in customer or user requirements, this is commonly known as:

A. Cost/benefit adjustments
B. Scope creep
C. Prototype issues
D. Expectations management

Answer: B

Explanation:
Reference:
http://www.umsl.edu/~sauterv/analysis/6840_f03_papers/gurlen/

NEW QUESTION 280
- (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 281
- (Exam Topic 5)
What is one key difference between Capital expenditures and Operating expenditures?

A. Operating expense cannot be written off while Capital expense can
B. Operating expenses can be depreciated over time and Capital expenses cannot
C. Capital expenses cannot include salaries and Operating expenses can
D. Capital expenditures allow for the cost to be depreciated over time and Operating does not

Answer: C

NEW QUESTION 285
- (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 288
- (Exam Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

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

Answer: A

NEW QUESTION 291
- (Exam Topic 5)
The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

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

Answer: B

NEW QUESTION 294
- (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 297
- (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 298
- (Exam Topic 5)
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.
What action should you take FIRST?

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

Answer: C

NEW QUESTION 299
- (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 300
- (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 301
- (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 305
- (Exam Topic 5)
Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.
To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

A. Business Impact Analysis
B. Business Continuity plan
C. Security roadmap
D. Annual report to shareholders

Answer: A

NEW QUESTION 306
- (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 307
- (Exam Topic 5)
SCENARIO: Critical servers show signs of erratic behavior within your organization’s intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security
Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.
What phase of the response provides measures to reduce the likelihood of an incident from recurring?

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

Answer: D

NEW QUESTION 309
- (Exam Topic 5)
Which of the following is an accurate statement regarding capital expenses?

A. They are easily reduced through the elimination of usage, such as reducing power for lighting of work areas during off-hours
B. Capital expenses can never be replaced by operational expenses
C. Capital expenses are typically long-term investments with value being realized through their use
D. The organization is typically able to regain the initial cost by selling this type of asset

Answer: A

NEW QUESTION 311
- (Exam Topic 5)
Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

A. Reviewing system administrator logs
B. Auditing configuration templates
C. Checking vendor product releases
D. Performing system scans

Answer: D

NEW QUESTION 312
- (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 314
- (Exam Topic 5)
As the Chief Information Security Officer, you are performing an assessment of security posture to understand what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows to detect and actively stop vulnerability exploits and attacks?

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

Answer: B

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

NEW QUESTION 317
- (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 321
- (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)
The process of creating a system which divides documents based on their security level to manage access to private data is known as

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

Answer: C

NEW QUESTION 327
- (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 328
- (Exam Topic 4)
Which of the following backup sites takes the longest recovery time?

A. Cold site
B. Hot site
C. Warm site
D. Mobile backup site

Answer: A

NEW QUESTION 330
- (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 333
- (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 338
- (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 341
- (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 344
- (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 349
- (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 354
- (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 357
- (Exam Topic 3)
The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong? (choose the BEST answer):

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

Answer: A

NEW QUESTION 361
- (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 362
- (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 364
- (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 366
- (Exam Topic 3)
What oversight should the information security team have in the change management process for application security?

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

Answer: C

NEW QUESTION 368
- (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 370
- (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 373
- (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 378
- (Exam Topic 3)
Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

A. Define the risk appetite
B. Determine budget constraints
C. Review project charters
D. Collaborate security projects

Answer: A

NEW QUESTION 379
- (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 383
- (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 388
- (Exam Topic 3)
Which of the following represents the BEST method of ensuring security program alignment to business needs?

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

Answer: B

NEW QUESTION 389
- (Exam Topic 3)
A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?

A. Poor audit support for the security program
B. A lack of executive presence within the security program
C. Poor alignment of the security program to business needs
D. This is normal since business units typically resist security requirements

Answer: C

NEW QUESTION 390
- (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 391
- (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 395
- (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 400
- (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 405
- (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 410
- (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 413
- (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 415
- (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 416
- (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 419
- (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 423
- (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 424
- (Exam Topic 2)
IT control objectives are useful to IT auditors as they provide the basis for understanding the:

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

Answer: A

NEW QUESTION 429
- (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 434
- (Exam Topic 2)
As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?

A. Nothing, this falls outside your area of influence.
B. Close and chain the door shut and send a company-wide memo banning the practice.
C. Have a risk assessment performed.
D. Post a guard at the door to maintain physical security

Answer: C

NEW QUESTION 438
- (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 442
- (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 443
- (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 447

- (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 450
- (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 452
- (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 453
- (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 458
- (Exam Topic 2)
Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

A. Meet regulatory compliance requirements
B. Better understand the threats and vulnerabilities affecting the environment
C. Better understand strengths and weaknesses of the program
D. Meet legal requirements

Answer: C

NEW QUESTION 461
- (Exam Topic 2)
Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

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

Answer: B

NEW QUESTION 464
- (Exam Topic 2)
Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

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

Answer: C

NEW QUESTION 466

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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