Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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

NEW QUESTION 1
- (Exam Topic 6)
What is the MOST critical output of the incident response process?

A. A complete document of all involved team members and the support they provided
B. Recovery of all data from affected systems
C. Lessons learned from the incident, so they can be incorporated into the incident response processes
D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: C

Explanation:
Reference: https://www.eccouncil.org/incident-response-plan-phases/

NEW QUESTION 2
- (Exam Topic 6)
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)
A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP). In developing the business impact assessment (BIA), which of the following MOST closely relate to the data
backup and restoral?

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

Answer: C

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

NEW QUESTION 4
- (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 5
- (Exam Topic 6)
When performing a forensic investigation, what are the two MOST common data sources for obtaining evidence from a computer and mobile devices?

A. RAM and unallocated space
B. Unallocated space and RAM
C. Slack space and browser cache
D. Persistent and volatile data

Answer: D

Explanation:
Reference: https://study.com/academy/lesson/data-storage-formats-digital-forensics-devices-types.html

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

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

Answer: B

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

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (Exam Topic 2)
Which of the following activities is the MAIN purpose of the risk assessment process?

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

Answer: D

NEW QUESTION 10
- (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 13
- (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 15
- (Exam Topic 2)
When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

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

Answer: C

NEW QUESTION 19
- (Exam Topic 2)
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls

Answer: B

NEW QUESTION 22
- (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 24
- (Exam Topic 2)
Creating a secondary authentication process for network access would be an example of?

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

Answer: C

NEW QUESTION 26
- (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 27
- (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 31
- (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 35
- (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 39
- (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 41
- (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 45
- (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 47
- (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 48
- (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 53
- (Exam Topic 1)
A company wants to fill a Chief Information Security Officer position in the organization. They need to define
and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

A. Multiple certifications, strong technical capabilities and lengthy resume
B. Industry certifications, technical knowledge and program management skills
C. College degree, audit capabilities and complex project management
D. Multiple references, strong background check and industry certifications

Answer: B

NEW QUESTION 56
- (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 57
- (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 60
- (Exam Topic 1)
The Information Security Governance program MUST:

A. integrate with other organizational governance processes
B. support user choice for Bring Your Own Device (BYOD)
C. integrate with other organizational governance processes
D. show a return on investment for the organization

Answer: A

NEW QUESTION 65
- (Exam Topic 1)
Risk that remains after risk mitigation is known as

A. Persistent risk
B. Residual risk
C. Accepted risk
D. Non-tolerated risk

Answer: B

NEW QUESTION 68
- (Exam Topic 1)
You have implemented a new security control. Which of the following risk strategy options have you engaged in?

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

Answer: D

NEW QUESTION 71

- (Exam Topic 1)
A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

A. Compliance to the Payment Card Industry (PCI) regulations.
B. Alignment with financial reporting regulations for each country where they operate.
C. Alignment with International Organization for Standardization (ISO) standards.
D. Compliance with patient data protection regulations for each country where they operate.

Answer: D

NEW QUESTION 74
- (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 78
- (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 81
- (Exam Topic 1)
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

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

Answer: C

NEW QUESTION 83
- (Exam Topic 1)
Which of the following has the GREATEST impact on the implementation of an information security governance model?

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

Answer: D

NEW QUESTION 85
- (Exam Topic 1)
A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

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

Answer: A

NEW QUESTION 89
- (Exam Topic 1)
Which of the following should be determined while defining risk management strategies?

A. Organizational objectives and risk tolerance
B. Risk assessment criteria
C. IT architecture complexity
D. Enterprise disaster recovery plans

Answer: A

NEW QUESTION 91
- (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 93
- (Exam Topic 6)
You have been promoted to the CISO of a big-box retail store chain reporting to the Chief Information Officer (CIO). The CIO's first mandate to you is to develop a cybersecurity compliance framework that will meet all the store's compliance requirements.
Which of the following compliance standard is the MOST important to the organization?

A. The Federal Risk and Authorization Management Program (FedRAMP)
B. ISO 27002
C. NIST Cybersecurity Framework
D. Payment Card Industry (PCI) Data Security Standard (DSS)

Answer: D

Explanation:
Reference:
https://searchcompliance.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

NEW QUESTION 97
- (Exam Topic 6)
Many successful cyber-attacks currently include:

A. Phishing Attacks
B. Misconfigurations
C. Social engineering
D. All of these

Answer: C

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

NEW QUESTION 102
- (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 104
- (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 109
- (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 113
- (Exam Topic 6)
What is a key policy that should be part of the information security plan?

A. Account management policy
B. Training policy
C. Acceptable Use policy
D. Remote Access policy

Answer: C

Explanation:
Reference: https://www.exabeam.com/information-security/information-security-policy/

NEW QUESTION 114
- (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 118
- (Exam Topic 5)
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. Recently, members of your organization have been targeted through a number of sophisticated phishing attempts and have compromised their system credentials.
What action can you take to prevent the misuse of compromised credentials to change bank account information from outside your organization while still allowing employees to manage their bank information?

A. Turn off VPN access for users originating from outside the country
B. Enable monitoring on the VPN for suspicious activity
C. Force a change of all passwords
D. Block access to the Employee-Self Service application via VPN

Answer: D

NEW QUESTION 123
- (Exam Topic 5)
Which of the following best describes the sensors designed to project and detect a light beam across an area?

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

Answer: D

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

NEW QUESTION 126
- (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 127
- (Exam Topic 5)
What is the primary reason for performing a return on investment analysis?

A. To decide between multiple vendors
B. To decide is the solution costs less than the risk it is mitigating
C. To determine the current present value of a project
D. To determine the annual rate of loss

Answer: B

NEW QUESTION 130
- (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 134
- (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 would be the FIRST step when addressing Information Security formally and consistently in this organization?

A. Contract a third party to perform a security risk assessment
B. Define formal roles and responsibilities for Internal audit functions
C. Define formal roles and responsibilities for Information Security
D. Create an executive security steering committee

Answer: C

NEW QUESTION 139
- (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 144
- (Exam Topic 5)
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.
Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

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

Answer: A

NEW QUESTION 146
- (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 147
- (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 150
- (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 151
- (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 152
- (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 153
- (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 158
- (Exam Topic 5)
A newly-hired CISO needs to understand the organization's financial management standards for business units and operations. Which of the following would be the best source of this information?

A. The internal accounting department
B. The Chief Financial Officer (CFO)

C. The external financial audit service
D. The managers of the accounts payables and accounts receivables teams

Answer: D

NEW QUESTION 162
- (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 166
- (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.
Symmetric encryption in general is preferable to asymmetric encryption when:

A. The number of unique communication links is large
B. The volume of data being transmitted is small
C. The speed of the encryption / deciphering process is essential
D. The distance to the end node is farthest away

Answer: C

NEW QUESTION 170
- (Exam Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

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

Answer: A

NEW QUESTION 171
- (Exam Topic 5)
What is the BEST reason for having a formal request for proposal process?

A. Creates a timeline for purchasing and budgeting
B. Allows small companies to compete with larger companies
C. Clearly identifies risks and benefits before funding is spent
D. Informs suppliers a company is going to make a purchase

Answer: C

NEW QUESTION 176
- (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 177
- (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 182

- (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 184
- (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 185
- (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 189
- (Exam Topic 5)
If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization. How would you prevent such type of attacks?

A. Conduct thorough background checks before you engage them
B. Hire the people through third-party job agencies who will vet them for you
C. Investigate their social networking profiles
D. It is impossible to block these attacks

Answer: A

NEW QUESTION 191
- (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 196
- (Exam Topic 5)
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.
Using the best business practices for project management you determine that the project correctly aligns with the company goals and the scope of the project is correct. What is the NEXT step?

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

Answer: C

NEW QUESTION 199
- (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 200
- (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 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.
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 207
- (Exam Topic 5)
Which of the following best describes an access control process that confirms the identity of the entity seeking access to a logical or physical area?

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

Answer: B

NEW QUESTION 212
- (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 213
- (Exam Topic 4)
The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?

A. Well established and defined digital forensics process
B. Establishing Enterprise-owned Botnets for preemptive attacks
C. Be able to retaliate under the framework of Active Defense
D. Collaboration with law enforcement

Answer: A

NEW QUESTION 215
- (Exam Topic 4)
The general ledger setup function in an enterprise resource package allows for setting accounting periods. Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

A. The need to change accounting periods on a regular basis.
B. The requirement to post entries for a closed accounting period.

C. The need to create and modify the chart of accounts and its allocations.
D. The lack of policies and procedures for the proper segregation of duties.

Answer: D

NEW QUESTION 216
- (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 220
- (Exam Topic 4)
What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

A. Traffic Analysis
B. Deep-Packet inspection
C. Packet sampling
D. Heuristic analysis

Answer: B

NEW QUESTION 224
- (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 226
- (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 230
- (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 231
- (Exam Topic 3)
Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

A. Risk Assessment
B. Incident Response
C. Risk Management
D. Network Security administration

Answer: C

NEW QUESTION 232
- (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 236
- (Exam Topic 3)
When is an application security development project complete?

A. When the application is retired.
B. When the application turned over to production.
C. When the application reaches the maintenance phase.
D. After one year.

Answer: A

NEW QUESTION 239
- (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 240
- (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 242
- (Exam Topic 3)
Your incident response plan should include which of the following?

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

Answer: C

NEW QUESTION 247
- (Exam Topic 3)
Which of the following represents the best method of ensuring business unit alignment with security program requirements?

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

Answer: C

NEW QUESTION 251
- (Exam Topic 3)
Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

A. Risk Management
B. Risk Assessment
C. System Testing

D. Vulnerability Assessment

Answer: B

NEW QUESTION 253
- (Exam Topic 3)
Which of the following is the MOST important component of any change management process?

A. Scheduling
B. Back-out procedures
C. Outage planning
D. Management approval

Answer: D

NEW QUESTION 257
- (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 259
- (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 263
- (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 265
- (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 270
- (Exam Topic 3)
Which of the following is the BEST indicator of a successful project?

A. it is completed on time or early as compared to the baseline project plan
B. it meets most of the specifications as outlined in the approved project definition
C. it comes in at or below the expenditures planned for in the baseline budget
D. the deliverables are accepted by the key stakeholders

Answer: D

NEW QUESTION 273
- (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 274
- (Exam Topic 3)
How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?

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

Answer: D

NEW QUESTION 276
- (Exam Topic 3)
Which of the following is a major benefit of applying risk levels?

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

Answer: B

NEW QUESTION 280
- (Exam Topic 3)
A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

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

Answer: D

NEW QUESTION 284
- (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 286
- (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 288
- (Exam Topic 2)
Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?

A. All vulnerabilities found on servers and desktops
B. Only critical and high vulnerabilities on servers and desktops
C. Only critical and high vulnerabilities that impact important production servers
D. All vulnerabilities that impact important production servers

Answer: C

NEW QUESTION 292
- (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 296
- (Exam Topic 2)
Which of the following are primary concerns for management with regard to assessing internal control objectives?

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

Answer: B

NEW QUESTION 299
- (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 304
- (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 305
- (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 308
- (Exam Topic 2)
With respect to the audit management process, management response serves what function?

A. placing underperforming units on notice for failing to meet standards
B. determining whether or not resources will be allocated to remediate a finding
C. adding controls to ensure that proper oversight is achieved by management
D. revealing the “root cause” of the process failure and mitigating for all internal and external units

Answer: B

NEW QUESTION 310
- (Exam Topic 2)
The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

A. The asset is more expensive than the remediation
B. The audit finding is incorrect
C. The asset being protected is less valuable than the remediation costs
D. The remediation costs are irrelevant; it must be implemented regardless of cost.

Answer: C

NEW QUESTION 311
- (Exam Topic 2)
During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

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

Answer: A

NEW QUESTION 315
- (Exam Topic 2)
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 317
- (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 319
- (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 324
- (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 326
- (Exam Topic 2)
The amount of risk an organization is willing to accept in pursuit of its mission is known as

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

Answer: C

NEW QUESTION 328
- (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 330
- (Exam Topic 2)
Which of the following illustrates an operational control process:

A. Classifying an information system as part of a risk assessment
B. Installing an appropriate fire suppression system in the data center
C. Conducting an audit of the configuration management process
D. Establishing procurement standards for cloud vendors

Answer: B

NEW QUESTION 332
- (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 333
- (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 338
- (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 343
- (Exam Topic 2)
Which represents PROPER separation of duties in the corporate environment?

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

Answer: D

NEW QUESTION 346
- (Exam Topic 2)
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

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

Answer: A

NEW QUESTION 350
- (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 351
- (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 355
.....

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