



EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

NEW QUESTION 1

- (Exam Topic 6)

An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO).

The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?

- A. ISO 22318 Supply Chain Continuity
- B. ISO 27031 BCM Readiness
- C. ISO 22301 BCM Requirements
- D. ISO 22317 BIA

Answer: C

Explanation:

Reference: <https://www.smartsheet.com/content/iso-22301-business-continuity-guide>

NEW QUESTION 2

- (Exam Topic 6)

What is the primary difference between regulations and standards?

- A. Standards will include regulations
- B. Standards that aren't followed are punishable by fines
- C. Regulations are made enforceable by the power provided by laws
- D. Regulations must be reviewed and approved by the business

Answer: C

NEW QUESTION 3

- (Exam Topic 6)

A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 4

- (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 5

- (Exam Topic 6)

What does RACI stand for?

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

Answer: C

Explanation:

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

NEW QUESTION 6

- (Exam Topic 6)

A bastion host should be placed:

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

Answer: C

Explanation:

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

NEW QUESTION 7

- (Exam Topic 6)

When managing a project, the MOST important activity in managing the expectations of stakeholders is:

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 8

- (Exam Topic 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 9

- (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 10

- (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 10

- (Exam Topic 2)

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

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

Answer: C

NEW QUESTION 11

- (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 12

- (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 15

- (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 17

- (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 21

- (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 24

- (Exam Topic 1)

Which of the following is the MOST important benefit of an effective security governance process?

- A. Reduction of liability and overall risk to the organization
- B. Better vendor management
- C. Reduction of security breaches
- D. Senior management participation in the incident response process

Answer: A

NEW QUESTION 27

- (Exam Topic 1)

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 31

- (Exam Topic 1)

The alerting, monitoring and life-cycle management of security related events is typically handled by the

- A. security threat and vulnerability management process
- B. risk assessment process
- C. risk management process
- D. governance, risk, and compliance tools

Answer: A

NEW QUESTION 34

- (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 36

- (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 41

- (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 45

- (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 48

- (Exam Topic 1)

Who is responsible for securing networks during a security incident?

- A. Chief Information Security Officer (CISO)
- B. Security Operations Center (SOC)
- C. Disaster Recovery (DR) manager
- D. Incident Response Team (IRT)

Answer: D

NEW QUESTION 51

- (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 54

- (Exam Topic 1)

Information security policies should be reviewed:

- A. by stakeholders at least annually
- B. by the CISO when new systems are brought online
- C. by the Incident Response team after an audit
- D. by internal audit semiannually

Answer: A

NEW QUESTION 58

- (Exam Topic 1)

According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

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

Answer: D

NEW QUESTION 63

- (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 65

- (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 68

- (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 72

- (Exam Topic 1)

Why is it vitally important that senior management endorse a security policy?

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

Answer: A

NEW QUESTION 77

- (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 78

- (Exam Topic 1)

Payment Card Industry (PCI) compliance requirements are based on what criteria?

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

Answer: D

NEW QUESTION 81

- (Exam Topic 6)

What are the common data hiding techniques used by criminals?

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

Answer: D

Explanation:

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

NEW QUESTION 85

- (Exam Topic 6)

What is an approach to estimating the strengths and weaknesses of alternatives used to determine options, which provide the BEST approach to achieving benefits while preserving savings called?

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

Answer: D

Explanation:

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

NEW QUESTION 87

- (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 88

- (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 92

- (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 94

- (Exam Topic 5)

Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs. When adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

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

Answer: D

NEW QUESTION 98

- (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 100

- (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 101

- (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 discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-facto implementation project?

- A. Create new use cases for operational use of the solution
- B. Determine if sufficient mitigating controls can be applied
- C. Decide to accept the risk on behalf of the impacted business units
- D. Report the deficiency to the audit team and create process exceptions

Answer: B

NEW QUESTION 104

- (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 106

- (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 107

- (Exam Topic 5)

Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.

Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

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

Answer: C

NEW QUESTION 112

- (Exam Topic 5)

The ability to demand the implementation and management of security controls on third parties providing services to an organization is

- A. Security Governance
- B. Compliance management
- C. Vendor management
- D. Disaster recovery

Answer: C

NEW QUESTION 115

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 119

- (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 121

- (Exam Topic 5)

SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning. Which of the following is the MOST logical next step?

- A. Validate the effectiveness of current controls
- B. Create detailed remediation funding and staffing plans
- C. Report the audit findings and remediation status to business stake holders
- D. Review security procedures to determine if they need modified according to findings

Answer: C

NEW QUESTION 125

- (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 129

- (Exam Topic 5)

The primary purpose of a risk register is to:

- A. Maintain a log of discovered risks
- B. Track individual risk assessments
- C. Develop plans for mitigating identified risks
- D. Coordinate the timing of scheduled risk assessments

Answer: A

Explanation:

Reference: <https://sitemate.com/us/resources/articles/safety/purpose-of-a-risk-register/>

NEW QUESTION 131

- (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 132

- (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 136

- (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 140

- (Exam Topic 5)

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

How can you reduce the administrative burden of distributing symmetric keys for your employer?

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

Answer: A

NEW QUESTION 141

- (Exam Topic 5)

What are the primary reasons for the development of a business case for a security project?

- A. To estimate risk and negate liability to the company
- B. To understand the attack vectors and attack sources

- C. To communicate risk and forecast resource needs
- D. To forecast usage and cost per software licensing

Answer: C

NEW QUESTION 145

- (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 147

- (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 150

- (Exam Topic 5)

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

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

Answer: B

NEW QUESTION 151

- (Exam Topic 5)

Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers."

Which group of people should be consulted when developing your security program?

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

Answer: D

NEW QUESTION 152

- (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 155

- (Exam Topic 5)

Which of the following is an accurate description of a balance sheet?

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

Answer: C

NEW QUESTION 159

- (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.

Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time. Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

- A. Security Guards posted outside the Data Center
- B. Data Loss Prevention (DLP)
- C. Rigorous syslog reviews
- D. Intrusion Detection Systems (IDS)

Answer: B

NEW QUESTION 160

- (Exam Topic 5)

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

- A. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door
- B. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
- C. Educate and enforce physical security policies of the company to all the employees on a regular basis
- D. Setup a mock video camera next to the special card reader adjacent to the secure door

Answer: C

NEW QUESTION 162

- (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 165

- (Exam Topic 5)

Which of the following is the MOST important reason for performing assessments of the security portfolio?

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

Answer: A

NEW QUESTION 167

- (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 171

- (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 174

- (Exam Topic 5)

A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website. This type of control is considered

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

Answer: C

NEW QUESTION 175

- (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 178

- (Exam Topic 5)

Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?

- A. Security regulations
- B. Asset classification
- C. Information security policy
- D. Data classification

Answer: C

NEW QUESTION 180

- (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 185

- (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 188

- (Exam Topic 5)

Which of the following would negatively impact a log analysis of a multinational organization?

- A. Centralized log management
- B. Encrypted log files in transit
- C. Each node set to local time
- D. Log aggregation agent each node

Answer: D

NEW QUESTION 193

- (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 197

- (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 202

- (Exam Topic 4)

Which of the following is the MAIN security concern for public cloud computing?

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

Answer: A

NEW QUESTION 203

- (Exam Topic 4)

What type of attack requires the least amount of technical equipment and has the highest success rate?

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

Answer: C

NEW QUESTION 204

- (Exam Topic 4)

An anonymity network is a series of?

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

Answer: D

NEW QUESTION 208

- (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 209

- (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 211

- (Exam Topic 4)

Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?

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

Answer: C

NEW QUESTION 216

- (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 217

- (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 220

- (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 222

- (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 225

- (Exam Topic 3)

In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

- A. Distance learning/Web seminars
- B. Formal Class
- C. One-One Training
- D. Self –Study (noncomputerized)

Answer: D

NEW QUESTION 227

- (Exam Topic 3)

A recommended method to document the respective roles of groups and individuals for a given process is to:

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

Answer: D

NEW QUESTION 231

- (Exam Topic 3)

Which of the following is considered one of the most frequent failures in project management?

- A. Overly restrictive management
- B. Excessive personnel on project
- C. Failure to meet project deadlines
- D. Insufficient resources

Answer: C

NEW QUESTION 232

- (Exam Topic 3)

Which of the following are not stakeholders of IT security projects?

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

Answer: B

NEW QUESTION 237

- (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 240

- (Exam Topic 3)

Risk appetite is typically determined by which of the following organizational functions?

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

Answer: C

NEW QUESTION 244

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 245

- (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 246

- (Exam Topic 3)

When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization. Which example below is the MOST creative way to maintain a strong security posture during these difficult times?

- A. Download open source security tools and deploy them on your production network
- B. Download trial versions of commercially available security tools and deploy on your production network
- C. Download open source security tools from a trusted site, test, and then deploy on production network
- D. Download security tools from a trusted source and deploy to production network

Answer: C

NEW QUESTION 250

- (Exam Topic 3)

Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

- A. Terms and Conditions
- B. Service Level Agreements (SLA)
- C. Statement of Work
- D. Key Performance Indicators (KPI)

Answer: B

NEW QUESTION 253

- (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 257

- (Exam Topic 3)

Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed. What can be done to ensure that security is addressed cost effectively?

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

Answer: D

NEW QUESTION 261

- (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 266

- (Exam Topic 2)

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

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

Answer: A

NEW QUESTION 269

- (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 270

- (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 275

- (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 279

- (Exam Topic 2)

The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is

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

Answer: B

NEW QUESTION 281

- (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 283

- (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 286

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * 712-50 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 712-50 Practice Test Here](#)