712-50 Dumps

EC-Council Certified CISO (CCISO)

https://www.certleader.com/712-50-dumps.html

NEW QUESTION 1
- (Topic 1)
A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

A. Enforce the existing security standards and do not allow the deployment of the new technology.
B. Amend the standard to permit the deployment.
C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Answer: C

NEW QUESTION 2
- (Topic 1)
An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

A. Data breach disclosure
B. Consumer right disclosure
C. Security incident disclosure
D. Special circumstance disclosure

Answer: A

NEW QUESTION 3
- (Topic 1)
Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

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

Answer: C

NEW QUESTION 4
- (Topic 1)
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. assessed by a business impact analysis.
B. protected under the information classification policy.
C. analyzed under the data ownership policy.
D. analyzed under the retention policy

Answer: D

NEW QUESTION 5
- (Topic 1)
You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

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

Answer: C

NEW QUESTION 6
- (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 7
- (Topic 1)
Who in the organization determines access to information?

A. Legal department

B. Compliance officer
C. Data Owner
D. Information security officer

Answer: C

NEW QUESTION 8
- (Topic 1)
Which of the following is the MOST important for a CISO to understand when identifying threats?

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

Answer: A

NEW QUESTION 9
- (Topic 1)
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer: A

NEW QUESTION 10
- (Topic 1)
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

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

Answer: B

NEW QUESTION 10
- (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 11
- (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 15
- (Topic 1)
After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

A. Risk Tolerance
B. Qualitative risk analysis
C. Risk Appetite
D. Quantitative risk analysis

Answer: D

NEW QUESTION 18
- (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 23
- (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 25
- (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 30
- (Topic 1)
A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

A. International Organization for Standardizations – 22301 (ISO-22301)
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27005 (ISO-27005)

Answer: A

NEW QUESTION 34
- (Topic 1)
A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?

A. Audit validation
B. Physical control testing
C. Compliance management
D. Security awareness training

Answer: C

NEW QUESTION 36
- (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 37
- (Topic 1)
An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System. Which of the following international standards can BEST assist this organization?

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

Answer: A

NEW QUESTION 38
- (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 40
- (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 43
- (Topic 1)
When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

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

Answer: :A

NEW QUESTION 46
- (Topic 2)
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

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

Answer: B

NEW QUESTION 49
- (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 54
- (Topic 2)
At which point should the identity access management team be notified of the termination of an employee?

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

Answer: C

NEW QUESTION 57
- (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 60
- (Topic 2)
Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?

A. Systems logs
B. Hardware error reports
C. Utilization reports
D. Availability reports

Answer: D

NEW QUESTION 63
- (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 66
- (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 70
- (Topic 2)
Creating a secondary authentication process for network access would be an example of?

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

Answer: A

NEW QUESTION 72
- (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 77
- (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 80
- (Topic 2)
You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis. Which of the following activities will help you in this?

A. Qualitative analysis

B. Quantitative analysis
C. Risk mitigation
D. Estimate activity duration

Answer: A

NEW QUESTION 81
- (Topic 2)
In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

A. Internal Audit
B. Database Administration
C. Information Security
D. Compliance

Answer: C

NEW QUESTION 84
- (Topic 2)
Dataflow diagrams are used by IT auditors to:

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

Answer: C

NEW QUESTION 87
- (Topic 2)
Which of the following activities results in change requests?

A. Preventive actions
B. Inspection
C. Defect repair
D. Corrective actions

Answer: A

NEW QUESTION 92
- (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 96
- (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 97
- (Topic 2)
An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:

A. Inform senior management of the risk involved.
B. Agree to work with the security officer on these shifts as a form of preventative control.
C. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
D. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.

Answer: :A

NEW QUESTION 98

- (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 102
- (Topic 2)
Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

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

Answer: C

NEW QUESTION 107
- (Topic 2)
Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

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

Answer: A

NEW QUESTION 109
- (Topic 2)
The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization's

A. Risk Management Program.
B. Anti-Spam controls.
C. Security Awareness Program.
D. Identity and Access Management Program.

Answer: C

NEW QUESTION 114
- (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 117
- (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 119
- (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 120
- (Topic 3)
Your company has a "no right to privacy" notice on all logon screens for your information
systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee's email account. What should you do? (choose the BEST answer):

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

Answer: B

NEW QUESTION 122
- (Topic 3)
When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

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

Answer: A

NEW QUESTION 123
- (Topic 3)
A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?

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

Answer: C

NEW QUESTION 124
- (Topic 3)
A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability. What do you do?

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

Answer: C

NEW QUESTION 125
- (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 129
- (Topic 3)
Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

A. Security administrators
B. Security mangers
C. Security technicians
D. Security analysts

Answer: :B

NEW QUESTION 133
- (Topic 3)
You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

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

Answer: B

NEW QUESTION 137
- (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 138
- (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 143
- (Topic 3)
Which of the following is considered a project versus a managed process?

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

Answer: D

NEW QUESTION 147
- (Topic 3)
An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents. Which of the following would be considered a MAJOR constraint for the
project?

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

Answer: C

NEW QUESTION 150
- (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 153
- (Topic 3)
Which of the following represents the BEST method of ensuring security program alignment to business needs?

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

Answer: B

NEW QUESTION 157
- (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 161
- (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 162
- (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 163
- (Topic 3)
A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state. Which of the following security issues is the MOST likely reason leading to the audit findings?

A. Lack of asset management processes
B. Lack of change management processes
C. Lack of hardening standards
D. Lack of proper access controls

Answer: B

NEW QUESTION 167
- (Topic 3)
Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

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

Answer: A

NEW QUESTION 169
- (Topic 3)
How often should the SSAE16 report of your vendors be reviewed?

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

Answer: C

NEW QUESTION 172
- (Topic 3)
An example of professional unethical behavior is:

A. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation
B. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
C. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
D. Storing client lists and other sensitive corporate internal documents on a removable thumb drive

Answer: C

NEW QUESTION 175
- (Topic 3)
When selecting a security solution with reoccurring maintenance costs after the first year (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 178
- (Topic 3)
You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do. What is the BEST approach to handle this situation?

A. Tell the team to do their best and respond to each alert
B. Tune the sensors to help reduce false positives so the team can react better
C. Request additional resources to handle the workload
D. Tell the team to only respond to the critical and high alerts

Answer: B

NEW QUESTION 179
- (Topic 4)
As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.
1.Covering tracks 2.Scanning and enumeration 3.Maintaining Access 4.Reconnaissance
5.Gaining Access

A. 4, 2, 5, 3, 1
B. 2, 5, 3, 1, 4
C. 4, 5, 2, 3, 1
D. 4, 3, 5, 2, 1

Answer: A

NEW QUESTION 184
- (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 186
- (Topic 4)
One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys should be used to encrypt the message?

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

Answer: C

NEW QUESTION 189
- (Topic 4)
Security related breaches are assessed and contained through which of the following?

A. The IT support team.
B. A forensic analysis.
C. Incident response
D. Physical security team.

Answer: C

NEW QUESTION 190
- (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 194
- (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 199
- (Topic 4)
The process for identifying, collecting, and producing digital information in support of legal proceedings is called

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

Answer: B

NEW QUESTION 203
- (Topic 4)
Which of the following statements about Encapsulating Security Payload (ESP) is true?

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

Answer: A

NEW QUESTION 207
- (Topic 4)
Your penetration testing team installs an in-line hardware key logger onto one of your
network machines. Which of the following is of major concern to the security organization?

A. In-line hardware keyloggers don't require physical access
B. In-line hardware keyloggers don't comply to industry regulations
C. In-line hardware keyloggers are undetectable by software
D. In-line hardware keyloggers are relatively inexpensive

Answer: C

NEW QUESTION 208
- (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 212
- (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 214
- (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 217
- (Topic 5)
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates. When multiple regulations or standards apply to your industry you should set controls to meet the:

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

Answer: A

NEW QUESTION 221
- (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 224
- (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 226
- (Topic 5)
As the CISO you need to write the IT security strategic plan. Which of the following is the MOST important to review before you start writing the plan?

A. The existing IT environment.
B. The company business plan.
C. The present IT budget.
D. Other corporate technology trends.

Answer: B

NEW QUESTION 229
- (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. The organization wants a more permanent solution to the threat to user credential compromise through phishing. What technical solution would BEST address this issue?

A. Professional user education on phishing conducted by a reputable vendor
B. Multi-factor authentication employing hard tokens
C. Forcing password changes every 90 days
D. Decreasing the number of employees with administrator privileges

Answer: B

NEW QUESTION 230
- (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 232
- (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 234
- (Topic 5)
Annual Loss Expectancy is derived from the function of which two factors?

A. Annual Rate of Occurrence and Asset Value
B. Single Loss Expectancy and Exposure Factor
C. Safeguard Value and Annual Rate of Occurrence
D. Annual Rate of Occurrence and Single Loss Expectancy

Answer: D

NEW QUESTION 238
- (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 240
- (Topic 5)
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.
Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

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

Answer: A

NEW QUESTION 242
- (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 247
- (Topic 5)
SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.
Which of the following is the FIRST action the CISO will perform after receiving the audit report?

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

Answer: B

NEW QUESTION 251
- (Topic 5)
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.
What action should you take FIRST?

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

Answer: C

NEW QUESTION 254
- (Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

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

Answer: :A

NEW QUESTION 255
- (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.
After determining the audit findings are accurate, which of the following is the MOST logical next activity?

A. Begin initial gap remediation analyses
B. Review the security organization's charter
C. Validate gaps with the Information Technology team
D. Create a briefing of the findings for executive management

Answer: A

NEW QUESTION 256
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 712-50 Exam with Our Prep Materials Via below:

https://www.certleader.com/712-50-dumps.html