EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

NEW QUESTION 1
- (Topic 1)
Which of the following is MOST likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

Answer: C

NEW QUESTION 2
- (Topic 1)
Risk is defined as:

A. Threat times vulnerability divided by control
B. Advisory plus capability plus vulnerability
C. Asset loss times likelihood of event
D. Quantitative plus qualitative impact

Answer: A

NEW QUESTION 3
- (Topic 1)
What is the definition of Risk in Information Security?

A. Risk = Probability x Impact
B. Risk = Threat x Probability
C. Risk = Financial Impact x Probability
D. Risk = Impact x Threat

Answer: A

NEW QUESTION 4
- (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 5
- (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 6
- (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 7
- (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 8
- (Topic 1)
What two methods are used to assess risk impact?

A. Cost and annual rate of expectance
B. Subjective and Objective
C. Qualitative and percent of loss realized
D. Quantitative and qualitative

Answer: D

NEW QUESTION 9
- (Topic 1)
Which of the following is considered the MOST effective tool against social engineering?

A. Anti-phishing tools
B. Anti-malware tools
C. Effective Security Vulnerability Management Program
D. Effective Security awareness program

Answer: D

NEW QUESTION 10
- (Topic 1)
A method to transfer risk is to:

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

Answer: C

NEW QUESTION 10
- (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 14
- (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 17
- (Topic 1)
When briefing senior management on the creation of a governance process, the MOST important aspect should be:

A. information security metrics.
B. knowledge required to analyze each issue.
C. baseline against which metrics are evaluated.
D. linkage to business area objectives.

Answer: D

NEW QUESTION 22
- (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 26
- (Topic 1)
Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

A. Strong authentication technologies
B. Financial reporting regulations
C. Credit card compliance and regulations
D. Local privacy laws

Answer: D

NEW QUESTION 29
- (Topic 1)
Which of the following has the GREATEST impact on the implementation of an information security governance model?

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

Answer: D

NEW QUESTION 32
- (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 35
- (Topic 1)
When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

A. How many credit card records are stored?
B. How many servers do you have?
C. What is the scope of the certification?
D. What is the value of the assets at risk?

Answer: C

NEW QUESTION 37
- (Topic 1)
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

A. Scan a representative sample of systems
B. Perform the scans only during off-business hours
C. Decrease the vulnerabilities within the scan tool settings
D. Filter the scan output so only pertinent data is analyzed

Answer: A

NEW QUESTION 42
- (Topic 1)
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

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

Answer: C

NEW QUESTION 46
- (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 51
- (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 52
- (Topic 1)
Ensuring that the actions of a set of people, applications and systems follow the organization’s rules is BEST described as:

A. Risk management
B. Security management
C. Mitigation management
D. Compliance management

Answer: D

NEW QUESTION 54
- (Topic 1)
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

A. National Institute for Standards and Technology 800-50 (NIST 800-50)
B. International Organization for Standardizations – 27005 (ISO-27005)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27004 (ISO-27004)

Answer: B

NEW QUESTION 58
- (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 59
- (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 63
- (Topic 2)
Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

A. Application logs
B. File integrity monitoring
C. SNMP traps
D. Syslog

Answer: B

NEW QUESTION 64
- (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 68
- (Topic 2)
You have implemented the new controls. What is the next step?

A. Document the process for the stakeholders
B. Monitor the effectiveness of the controls
C. Update the audit findings report
D. Perform a risk assessment

Answer: B

NEW QUESTION 69
- (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 74
- (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 79
- (Topic 2)
IT control objectives are useful to IT auditors as they provide the basis for understanding the:

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

Answer: A

NEW QUESTION 83
- (Topic 2)
Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

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

Answer: D

NEW QUESTION 88
- (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 93
- (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 94
- (Topic 2)
The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is consider a bad practice MAINLY because

A. The IT team is not familiar in IT audit practices
B. This represents a bad implementation of the Least Privilege principle
C. This represents a conflict of interest
D. The IT team is not certified to perform audits

Answer: C

NEW QUESTION 97
- (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 99
- (Topic 2)
Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

A. ISO 27001
B. ISO 27002
C. ISO 27004
D. ISO 27005

Answer: :D

NEW QUESTION 103
- (Topic 2)
An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application. What should be the NEXT step?

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

Answer: C

NEW QUESTION 107
- (Topic 2)
The risk found after a control has been fully implemented is called:

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

Answer: A

NEW QUESTION 108
- (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)
Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

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

Answer: B

NEW QUESTION 113
- (Topic 2)
Which of the following activities must be completed BEFORE you can calculate risk?

A. Determining the likelihood that vulnerable systems will be attacked by specific threats
B. Calculating the risks to which assets are exposed in their current setting
C. Assigning a value to each information asset
D. Assessing the relative risk facing the organization’s information assets

Answer: C

NEW QUESTION 115
- (Topic 2)
Which of the following is a fundamental component of an audit record?

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

Answer: A

NEW QUESTION 120
- (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 124
- (Topic 2)
The patching and monitoring of systems on a consistent schedule is required by?

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

Answer: C

NEW QUESTION 127
- (Topic 3)
Which of the following information may be found in table top exercises for incident response?

A. Security budget augmentation
B. Process improvements
C. Real-time to remediate
D. Security control selection

Answer: B

NEW QUESTION 128
- (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 131
- (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 133
- (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 137
- (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 139
- (Topic 3)
Which business stakeholder is accountable for the integrity of a new information system?

A. CISO
B. Compliance Officer
C. Project manager
D. Board of directors

Answer: A

NEW QUESTION 144
- (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 146
- (Topic 3)
Which of the following methodologies references the recommended industry standard that Information security project managers should follow?

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

Answer: D

NEW QUESTION 148
- (Topic 3)
The ultimate goal of an IT security projects is:

A. Increase stock value
B. Complete security
C. Support business requirements
D. Implement information security policies

Answer: C

NEW QUESTION 150
- (Topic 3)
Which of the following represents the best method of ensuring business unit alignment with security program requirements?

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

Answer: C

NEW QUESTION 151
- (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 156
- (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 160
- (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 161
- (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 164
- (Topic 3)
Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

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

Answer: C

NEW QUESTION 166
- (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 170
- (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 175
- (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 177
- (Topic 3)
Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement. What type of risk tolerance is Acme exhibiting? (choose the BEST answer):

A. low risk-tolerance
B. high risk-tolerance
C. moderate risk-tolerance
D. medium-high risk-tolerance

Answer: A

NEW QUESTION 180
- (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 182
- (Topic 3)
When should IT security project management be outsourced?

A. When organizational resources are limited
B. When the benefits of outsourcing outweigh the inherent risks of outsourcing
C. On new, enterprise-wide security initiatives
D. On projects not forecasted in the yearly budget

Answer: B

NEW QUESTION 185

- (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 189
- (Topic 3)
A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets. This demonstrates which of the following principles?

A. Security alignment to business goals
B. Regulatory compliance effectiveness
C. Increased security program presence
D. Proper organizational policy enforcement

Answer: A

NEW QUESTION 192
- (Topic 3)
Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

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

Answer: B

NEW QUESTION 196
- (Topic 4)
Which wireless encryption technology makes use of temporal keys?

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

Answer: B

NEW QUESTION 197
- (Topic 4)
Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the incident handling process will utilize the signature to resolve this incident?

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

Answer: D

NEW QUESTION 200
- (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 201
- (Topic 4)
Which of the following is a countermeasure to prevent unauthorized database access from web applications?

A. Session encryption
B. Removing all stored procedures
C. Input sanitization
D. Library control

Answer: C

NEW QUESTION 204
- (Topic 4)
SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 207
- (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 209
- (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 210
- (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 215
- (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 216
- (Topic 4)
Which of the following backup sites takes the longest recovery time?

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

Answer: A

NEW QUESTION 221
- (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 224
- (Topic 4)
What is the FIRST step in developing the vulnerability management program?

A. Baseline the Environment
B. Maintain and Monitor
C. Organization Vulnerability
D. Define Policy

Answer: A

NEW QUESTION 226
- (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 227
- (Topic 5)
When updating the security strategic planning document what two items must be included?

A. Alignment with the business goals and the vision of the CIO
B. The risk tolerance of the company and the company mission statement
C. The executive summary and vision of the board of directors
D. The alignment with the business goals and the risk tolerance

Answer: D

NEW QUESTION 228
- (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 230
- (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 232
- (Topic 5)
The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

A. Security certification
B. Security system analysis
C. Security accreditation

D. Alignment with business practices and goals.

Answer: C

NEW QUESTION 236
- (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 241
- (Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?

A. Lack of risk management process
B. Lack of sponsorship from executive management
C. IT security centric agenda
D. Compliance centric agenda

Answer: C

NEW QUESTION 246
- (Topic 5)
When creating contractual agreements and procurement processes why should security requirements be included?

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

Answer: B

NEW QUESTION 250
- (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 251
- (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 253
- (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 257
- (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 formulating the remediation plan, what is a required input?

A. Board of directors
B. Risk assessment
C. Patching history
D. Latest virus definitions file

Answer: B

NEW QUESTION 259
- (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 260
- (Topic 5)
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.
Using the best business practices for project management you determine that the project correct aligns with the company goals. What needs to be verified FIRST?

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

Answer: A

NEW QUESTION 265
- (Topic 5)
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
What is one proven method to account for common elements found within separate
regulations and/or standards?

A. Hire a GRC expert
B. Use the Find function of your word processor
C. Design your program to meet the strictest government standards
D. Develop a crosswalk

Answer: D

NEW QUESTION 270
- (Topic 5)
Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

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

Answer: A

NEW QUESTION 273
- (Topic 5)
File Integrity Monitoring (FIM) is considered a

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

Answer: C

NEW QUESTION 277
- (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 282
- (Topic 5)
When dealing with risk, the information security practitioner may choose to:

A. assign
B. transfer
C. acknowledge
D. defer

Answer: C

NEW QUESTION 285
- (Topic 5)
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN.
Once supervisors and data owners have approved requests, information system administrators will implement

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

Answer: A

NEW QUESTION 289
- (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 290
- (Topic 5)
Which of the following is MOST useful when developing a business case for security initiatives?

A. Budget forecasts
B. Request for proposals
C. Cost/benefit analysis
D. Vendor management

Answer: C

NEW QUESTION 294
......