

## 712-50 Dumps

### EC-Council Certified CISO (CCISO)

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



#### NEW QUESTION 1

- (Topic 1)

A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

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

**Answer:** A

#### NEW QUESTION 2

- (Topic 1)

A global retail company is creating a new compliance management process. Which of the following regulations is of MOST importance to be tracked and managed by this process?

- A. Information Technology Infrastructure Library (ITIL)
- B. International Organization for Standardization (ISO) standards
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. National Institute for Standards and Technology (NIST) standard

**Answer:** C

#### NEW QUESTION 3

- (Topic 1)

You have implemented a new security control. Which of the following risk strategy options have you engaged in?

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

**Answer:** D

#### NEW QUESTION 4

- (Topic 1)

Which of the following provides an audit framework?

- A. Control Objectives for IT (COBIT)
- B. Payment Card Industry-Data Security Standard (PCI-DSS)
- C. International Organization Standard (ISO) 27002
- D. National Institute of Standards and Technology (NIST) SP 800-30

**Answer:** :A

#### NEW QUESTION 5

- (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 6

- (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 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)

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 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)

An organization information security policy serves to

- A. establish budgetary input in order to meet compliance requirements
- B. establish acceptable systems and user behavior
- C. define security configurations for systems
- D. define relationships with external law enforcement agencies

**Answer:** B

**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 15**

- (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 16**

- (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 17**

- (Topic 1)

Which of the following is a critical operational component of an Incident Response Program (IRP)?

- A. Weekly program budget reviews to ensure the percentage of program funding remains constant.

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

**Answer:** C

**NEW QUESTION 20**

- (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 22**

- (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 25**

- (Topic 1)

Developing effective security controls is a balance between:

- A. Risk Management and Operations
- B. Corporate Culture and Job Expectations
- C. Operations and Regulations
- D. Technology and Vendor Management

**Answer:** A

**NEW QUESTION 29**

- (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**

- (Topic 1)

An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?

- A. Determine the risk tolerance
- B. Perform an asset classification
- C. Create an architecture gap analysis
- D. Analyze existing controls on systems

**Answer:** B

**NEW QUESTION 38**

- (Topic 1)

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

- A. Threat
- B. Vulnerability
- C. Attack vector
- D. Exploitation

**Answer:** B

**NEW QUESTION 41**

- (Topic 1)

When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

- A. Escalation
- B. Recovery
- C. Eradication
- D. Containment

**Answer: D**

#### NEW QUESTION 46

- (Topic 1)

A security manager regularly checks work areas after business 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 50

- (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)

The Information Security Management program MUST protect:

- A. all organizational assets
- B. critical business processes and /or revenue streams
- C. intellectual property released into the public domain
- D. against distributed denial of service attacks

**Answer: B**

#### NEW QUESTION 55

- (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 58

- (Topic 1)

Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

- A. Security officer
- B. Data owner
- C. Vulnerability engineer
- D. System administrator

**Answer: D**

#### NEW QUESTION 60

- (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 64**

- (Topic 1)

A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected. Who must be informed of this incident?

- A. Internal audit
- B. The data owner
- C. All executive staff
- D. Government regulators

**Answer: B**

**NEW QUESTION 66**

- (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 67**

- (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 71**

- (Topic 2)

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

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

**Answer: B**

**NEW QUESTION 73**

- (Topic 2)

Which of the following is a benefit of a risk-based approach to audit planning?

- A. Resources are allocated to the areas of the highest concern
- B. Scheduling may be performed months in advance
- C. Budgets are more likely to be met by the IT audit staff
- D. Staff will be exposed to a variety of technologies

**Answer: A**

**NEW QUESTION 77**

- (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 81**

- (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 86**

- (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 87**

- (Topic 2)

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees. Which of the following can be used as a KPI?

- A. Number of callers who report security issues.
- B. Number of callers who report a lack of customer service from the call center
- C. Number of successful social engineering attempts on the call center
- D. Number of callers who abandon the call before speaking with a representative

**Answer:** C

**NEW QUESTION 88**

- (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 91**

- (Topic 2)

When you develop your audit remediation plan what is the MOST important criteria?

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

**Answer:** C

**NEW QUESTION 92**

- (Topic 2)

Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

- A. It allows executives to more effectively monitor IT implementation costs
- B. Implementation of it eases an organization's auditing and compliance burden
- C. Information Security (IS) procedures often require augmentation with other standards
- D. It provides for a consistent and repeatable staffing model for technology organizations

**Answer:** B

**NEW QUESTION 94**

- (Topic 2)

Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

- A. Security Administrators
- B. Internal/External Audit
- C. Risk Management
- D. Security Operations

**Answer:** B

**NEW QUESTION 98**

- (Topic 2)

When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

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

**Answer:** A

**NEW QUESTION 100**

- (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 105**

- (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 109**

- (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 110**

- (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 112**

- (Topic 2)

Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

- A. Control Objective for Information Technology (COBIT)
- B. Committee of Sponsoring Organizations (COSO)
- C. Payment Card Industry (PCI)
- D. Information Technology Infrastructure Library (ITIL)

**Answer:** A

**NEW QUESTION 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 118**



- (Topic 2)

Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

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

**Answer: C**

#### NEW QUESTION 121

- (Topic 2)

During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

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

**Answer: A**

#### NEW QUESTION 124

- (Topic 2)

An organization has implemented a change management process for all changes to the IT production environment. This change management process follows best practices and is expected to help stabilize the availability and integrity of the organization's IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process:

- A. Number of change orders rejected
- B. Number and length of planned outages
- C. Number of unplanned outages
- D. Number of change orders processed

**Answer: C**

#### NEW QUESTION 126

- (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 129

- (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 130

- (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 134

- (Topic 3)

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

- A. Cost benefit
- B. Risk appetite
- C. Business continuity
- D. Likelihood of impact

**Answer:** :B

**NEW QUESTION 138**

- (Topic 3)

When managing the critical path of an IT security project, which of the following is MOST important?

- A. Knowing who all the stakeholders are.
- B. Knowing the people on the data center team.
- C. Knowing the threats to the organization.
- D. Knowing the milestones and timelines of deliverables.

**Answer:** :D

**NEW QUESTION 142**

- (Topic 3)

When entering into a third party vendor agreement for security services, at what point in the process is it BEST to understand and validate the security posture and compliance level of the vendor?

- A. At the time the security services are being performed and the vendor needs access to the network
- B. Once the agreement has been signed and the security vendor states that they will need access to the network
- C. Once the vendor is on premise and before they perform security services
- D. Prior to signing the agreement and before any security services are being performed

**Answer:** D

**NEW QUESTION 144**

- (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 149**

- (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 152**

- (Topic 3)

The company decides to release the application without remediating the high-risk vulnerabilities. Which of the following is the MOST likely reason for the company to release the application?

- A. The company lacks a risk management process
- B. The company does not believe the security vulnerabilities to be real
- C. The company has a high risk tolerance
- D. The company lacks the tools to perform a vulnerability assessment

**Answer:** C

**NEW QUESTION 157**

- (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 159**

- (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 164**

- (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 165**

- (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 166**

- (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 167**

- (Topic 3)

Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

- A. System testing
- B. Risk assessment
- C. Incident response
- D. Planning

**Answer: A**

**NEW QUESTION 172**

- (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 173**

- (Topic 3)

Which of the following is the MOST important component of any change management process?

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

**Answer:** D

**NEW QUESTION 175**

- (Topic 3)

When is an application security development project complete?

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

**Answer:** A

**NEW QUESTION 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 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 183**

- (Topic 3)

Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

- A. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
- B. Create separate controls for the business units based on the types of business and functions they perform
- C. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
- D. Provide the business units with control mandates and schedules of audits for compliance validation

**Answer:** C

**NEW QUESTION 185**

- (Topic 4)

Your organization provides open guest wireless access with no captive portals. What can you do to assist with law enforcement investigations if one of your guests is suspected of committing an illegal act using your network?

- A. Configure logging on each access point
- B. Install a firewall software on each wireless access point.
- C. Provide IP and MAC address
- D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.

**Answer:** :C

**NEW QUESTION 190**

- (Topic 4)

The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?

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

**Answer:** A

**NEW QUESTION 192**

- (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 196**

- (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 200**

- (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 205**

- (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 210**

- (Topic 4)

Which of the following is a symmetric encryption algorithm?

- A. 3DES
- B. MD5
- C. ECC
- D. RSA

**Answer:** A

**NEW QUESTION 211**

- (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 214**

- (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)

Physical security measures typically include which of the following components?

- A. Physical, Technical, Operational
- B. Technical, Strong Password, Operational
- C. Operational, Biometric, Physical
- D. Strong password, Biometric, Common Access Card

**Answer:** A

#### NEW QUESTION 218

- (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 223

- (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 224

- (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 225

- (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. This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?

- A. International encryption restrictions
- B. Compliance to Payment Card Industry (PCI) data security standards
- C. Compliance with local government privacy laws
- D. Adherence to local data breach notification laws

**Answer:** B

#### NEW QUESTION 229

- (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 234

- (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: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.

An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

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

**Answer:** A

#### NEW QUESTION 240

- (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 241

- (Topic 5)

You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.

Using the best business practices for project management you determine that the project correctly aligns with the company goals and the scope of the project is correct. What is the NEXT step?

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

**Answer:** C

#### NEW QUESTION 246

- (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 249

- (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 251

- (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 256

- (Topic 5)

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years. The organization has already been subject to a significant amount of credit card fraud. Which of the following is the MOST likely reason for this fraud?

- A. Lack of compliance to the Payment Card Industry (PCI) standards
- B. Ineffective security awareness program
- C. Security practices not in alignment with ISO 27000 frameworks
- D. Lack of technical controls when dealing with credit card data

**Answer:** A

#### NEW QUESTION 259

- (Topic 5)

Human resource planning for security professionals in your organization is a:

- A. Simple and easy task because the threats are getting easier to find and correct.
- B. Training requirement that is met through once every year user training.
- C. Training requirement that is on-going and always changing.
- D. Not needed because automation and anti-virus software has eliminated the threats.

**Answer:** C

#### NEW QUESTION 263

- (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 267

- (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 269

- (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 272

- (Topic 5)

When analyzing and forecasting a capital expense budget what are not included?

- A. Network connectivity costs
- B. New datacenter to operate from

- C. Upgrade of mainframe
- D. Purchase of new mobile devices to improve operations

**Answer:** A

#### NEW QUESTION 273

- (Topic 5)

The new CISO was informed of all the Information Security projects that the organization has in progress. Two projects are over a year behind schedule and over budget. Using best business practices for project management you determine that the project correctly aligns with the company goals. Which of the following needs to be performed NEXT?

- A. Verify the scope of the project
- B. Verify the regulatory requirements
- C. Verify technical resources
- D. Verify capacity constraints

**Answer:** C

#### NEW QUESTION 275

- (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 277

- (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 281

- (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 282

- (Topic 5)

Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.

Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

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

**Answer:** A

#### NEW QUESTION 283

- (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 288**

- (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 293**

.....

## 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>