

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)

Which of the following is MOST likely to be discretionary?

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

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)

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 6

- (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 7

- (Topic 1)

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

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

Answer: A

NEW QUESTION 8

- (Topic 1)

Which of the following most commonly falls within the scope of an information security governance steering committee?

- A. Approving access to critical financial systems
- B. Developing content for security awareness programs
- C. Interviewing candidates for information security specialist positions
- D. Vetting information security policies

Answer: D

NEW QUESTION 9

- (Topic 1)

Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

- A. Need to comply with breach disclosure laws
- B. Need to transfer the risk associated with hosting PII data
- C. Need to better understand the risk associated with using PII data
- D. Fiduciary responsibility to safeguard credit card information

Answer: C

NEW QUESTION 10

- (Topic 1)

The success of the Chief Information Security Officer is MOST dependent upon:

- A. favorable audit findings
- B. following the recommendations of consultants and contractors
- C. development of relationships with organization executives
- D. raising awareness of security issues with end users

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 12

- (Topic 1)

What is the first thing that needs to be completed in order to create a security program for your organization?

- A. Risk assessment
- B. Security program budget
- C. Business continuity plan
- D. Compliance and regulatory analysis

Answer: A

NEW QUESTION 17

- (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 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 23

- (Topic 1)

Which of the following is MOST important when dealing with an Information Security Steering committee:

- A. Include a mix of members from different departments and staff levels.
- B. Ensure that security policies and procedures have been vetted and approved.
- C. Review all past audit and compliance reports.
- D. Be briefed about new trends and products at each meeting by a vendor.

Answer: C

NEW QUESTION 25

- (Topic 1)

What is the MAIN reason for conflicts between Information Technology and Information Security programs?

- A. Technology governance defines technology policies and standards while security governance does not.
- B. Security governance defines technology best practices and Information Technology governance does not.
- C. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
- D. The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.

Answer: D

NEW QUESTION 30

- (Topic 1)

What is the main purpose of the Incident Response Team?

- A. Ensure efficient recovery and reinstate repaired systems
- B. Create effective policies detailing program activities
- C. Communicate details of information security incidents
- D. Provide current employee awareness programs

Answer: A

NEW QUESTION 31

- (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 low

Answer: C

NEW QUESTION 34

- (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 39

- (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 44

- (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 45

- (Topic 1)

When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

- A. In promiscuous mode and only detect malicious traffic.
- B. In-line and turn on blocking mode to stop malicious traffic.
- C. In promiscuous mode and block malicious traffic.
- D. In-line and turn on alert mode to stop malicious traffic.

Answer: B

NEW QUESTION 47

- (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 49

- (Topic 1)

A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

- A. Lack of a formal security awareness program
- B. Lack of a formal security policy governance process
- C. Lack of formal definition of roles and responsibilities
- D. Lack of a formal risk management policy

Answer: B

NEW QUESTION 51

- (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 56

- (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 60

- (Topic 2)

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

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

Answer: B

NEW QUESTION 64

- (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 68

- (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 69

- (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 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)

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 84

- (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)

Which of the following are primary concerns for management with regard to assessing internal control objectives?

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

D. Confidentiality, Compliance, Cost

Answer: B

NEW QUESTION 90

- (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 93

- (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 97

- (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 104

- (Topic 2)

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

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

Answer: C

NEW QUESTION 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 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 116

- (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 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 126

- (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 130

- (Topic 2)

The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

- A. assign the responsibility to the information security team.
- B. assign the responsibility to the team responsible for the management of the controls.
- C. create operational reports on the effectiveness of the controls.
- D. perform an independent audit of the security controls.

Answer: D

NEW QUESTION 132

- (Topic 2)

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

- A. Risk metrics
- B. Management metrics
- C. Operational metrics
- D. Compliance metrics

Answer: C

NEW QUESTION 136

- (Topic 3)

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

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

Answer: C

NEW QUESTION 141

- (Topic 3)

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

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

Answer: C

NEW QUESTION 144

- (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 146

- (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 147

- (Topic 3)

A stakeholder is a person or group:

- A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
- B. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
- C. That has budget authority.
- D. That will ultimately use the system.

Answer: A

NEW QUESTION 148

- (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 149

- (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 155

- (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 159

- (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 164

- (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 169

- (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 170

- (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 175

- (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 180

- (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 184

- (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 188

- (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 193

- (Topic 4)

Which of the following is a symmetric encryption algorithm?

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

Answer: A

NEW QUESTION 195

- (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 197

- (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 198

- (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 200

- (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 202

- (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 205

- (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 209

- (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.

The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization. From an organizational perspective, which of the following is the LIKELY reason for this?

- A. The CISO does not report directly to the CEO of the organization
- B. The CISO reports to the IT organization
- C. The CISO has not implemented a policy management framework
- D. The CISO has not implemented a security awareness program

Answer: B

NEW QUESTION 210

- (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 211

- (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 216

- (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 219

- (Topic 5)

Which of the following provides an independent assessment of a vendor's internal security controls and overall posture?

- A. Alignment with business goals
- B. ISO27000 accreditation
- C. PCI attestation of compliance
- D. Financial statements

Answer: B

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.

In what phase of the response will the team extract information from the affected systems without altering original data?

- A. Response
- B. Investigation
- C. Recovery
- D. Follow-up

Answer: B

NEW QUESTION 225

- (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 228

- (Topic 5)

What is the primary reason for performing vendor management?

- A. To understand the risk coverage that are being mitigated by the vendor
- B. To establish a vendor selection process
- C. To document the relationship between the company and the vendor
- D. To define the partnership for long-term success

Answer: A

NEW QUESTION 232

- (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 236

- (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 238

- (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 243

- (Topic 5)

The total cost of security controls should:

- A. Be equal to the value of the information resource being protected
- B. Be greater than the value of the information resource being protected
- C. Be less than the value of the information resource being protected
- D. Should not matter, as long as the information resource is protected

Answer: C

NEW QUESTION 245

- (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 248

- (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 251

- (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 256

- (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 261

- (Topic 5)

SCENARIO: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.

What phase of the response provides measures to reduce the likelihood of an incident from recurring?

- A. Response
- B. Investigation
- C. Recovery
- D. Follow-up

Answer: D

NEW QUESTION 266

- (Topic 5)

Acceptable levels of information security risk tolerance in an organization should be determined by?

- A. Corporate legal counsel
- B. CISO with reference to the company goals
- C. CEO and board of director
- D. Corporate compliance committee

Answer: C

NEW QUESTION 267

- (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 272

.....

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>