

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

<https://www.2passeasy.com/dumps/712-50/>



NEW QUESTION 1

- (Topic 1)

Regulatory requirements typically force organizations to implement

- A. Mandatory controls
- B. Discretionary controls
- C. Optional controls
- D. Financial controls

Answer: A

NEW QUESTION 2

- (Topic 1)

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

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

Answer: C

NEW QUESTION 3

- (Topic 1)

Which of the following intellectual Property components is focused on maintaining brand recognition?

- A. Trademark
- B. Patent
- C. Research Logs
- D. Copyright

Answer: A

NEW QUESTION 4

- (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 5

- (Topic 1)

Information security policies should be reviewed:

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

Answer: A

NEW QUESTION 6

- (Topic 1)

You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

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

Answer: C

NEW QUESTION 7

- (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 8

- (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 9

- (Topic 1)

What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

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

Answer: B

NEW QUESTION 10

- (Topic 1)

When choosing a risk mitigation method what is the MOST important factor?

- A. Approval from the board of directors
- B. Cost of the mitigation is less than the risk
- C. Metrics of mitigation method success
- D. Mitigation method complies with PCI regulations

Answer: B

NEW QUESTION 10

- (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 14

- (Topic 1)

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

- A. Multiple certifications, strong technical capabilities and lengthy resume
- B. Industry certifications, technical knowledge and program management skills
- C. College degree, audit capabilities and complex project management
- D. Multiple references, strong background check and industry certifications

Answer: B

NEW QUESTION 17

- (Topic 1)

The PRIMARY objective for information security program development should be:

- A. Reducing the impact of the risk to the business.
- B. Establishing strategic alignment with business continuity requirements
- C. Establishing incident response programs.
- D. Identifying and implementing the best security solutions.

Answer: A

NEW QUESTION 20

- (Topic 1)

What is the relationship between information protection and regulatory compliance?

- A. That all information in an organization must be protected equally.

- B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
- C. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.
- D. There is no relationship between the two.

Answer: C

NEW QUESTION 21

- (Topic 1)

An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

- A. A high threat environment
- B. A low risk tolerance environment
- C. A low vulnerability environment
- D. A high risk tolerance environment

Answer: D

NEW QUESTION 25

- (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 27

- (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 32

- (Topic 1)

Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

- A. Poses a strong technical background
- B. Understand all regulations affecting the organization
- C. Understand the business goals of the organization
- D. Poses a strong auditing background

Answer: C

NEW QUESTION 33

- (Topic 1)

When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

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

Answer: A

NEW QUESTION 38

- (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 43

- (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 48

- (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 51

- (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 55

- (Topic 2)

Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

- A. Lack of notification to the public of disclosure of confidential information.
- B. Lack of periodic examination of access rights
- C. Failure to notify police of an attempted intrusion
- D. Lack of reporting of a successful denial of service attack on the network.

Answer: A

NEW QUESTION 57

- (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 58

- (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 60

- (Topic 2)

You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

- A. Validate that security awareness program content includes information about the potential vulnerability
- B. Conduct a thorough risk assessment against the current implementation to determine system functions
- C. Determine program ownership to implement compensating controls

D. Send a report to executive peers and business unit owners detailing your suspicions

Answer: B

NEW QUESTION 62

- (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 65

- (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 69

- (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 74

- (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 78

- (Topic 2)

The effectiveness of an audit is measured by?

- A. The number of actionable items in the recommendations
- B. How it exposes the risk tolerance of the company
- C. How the recommendations directly support the goals of the company
- D. The number of security controls the company has in use

Answer: C

NEW QUESTION 83

- (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 87

- (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 91

- (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 92

- (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 93

- (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 96

- (Topic 2)

As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?

- A. Nothing, this falls outside your area of influence.
- B. Close and chain the door shut and send a company-wide memo banning the practice.
- C. Have a risk assessment performed.
- D. Post a guard at the door to maintain physical security

Answer: C

NEW QUESTION 101

- (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 105

- (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 107

- (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 108

- (Topic 3)

You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

- A. Risk averse
- B. Risk tolerant
- C. Risk conditional
- D. Risk minimal

Answer: B

NEW QUESTION 111

- (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 113

- (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 114

- (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 116

- (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 117

- (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 118

- (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 123

- (Topic 3)

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

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

Answer: B

NEW QUESTION 127

- (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 132

- (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 137

- (Topic 3)

An application vulnerability assessment has identified a security flaw in an application. This is a flaw that was previously identified and remediated on a prior release of the application. Which of the following is MOST likely the reason for this recurring issue?

- A. Ineffective configuration management controls
- B. Lack of change management controls
- C. Lack of version/source controls
- D. High turnover in the application development department

Answer: C

NEW QUESTION 140

- (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 144

- (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 148

- (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 151

- (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 154

- (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 156

- (Topic 3)

When selecting a security solution with reoccurring maintenance costs after the first year (choose the BEST answer):

- A. The CISO should cut other essential programs to ensure the new solution's continued use
- B. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
- C. Defer selection until the market improves and cash flow is positive
- D. Implement the solution and ask for the increased operating cost budget when it is time

Answer: B

NEW QUESTION 160

- (Topic 3)

Which of the following is critical in creating a security program aligned with an organization's goals?

- A. Ensure security budgets enable technical acquisition and resource allocation based on internal compliance requirements
- B. Develop a culture in which users, managers and IT professionals all make good decisions about information risk
- C. Provide clear communication of security program support requirements and audit schedules
- D. Create security awareness programs that include clear definition of security program goals and charters

Answer: B

NEW QUESTION 163

- (Topic 4)

The process of identifying and classifying assets is typically included in the

- A. Threat analysis process
- B. Asset configuration management process
- C. Business Impact Analysis
- D. Disaster Recovery plan

Answer: C

NEW QUESTION 167

- (Topic 4)

As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.

1.Covering tracks 2.Scanning and enumeration 3.Maintaining Access 4.Reconnaissance
5.Gaining Access

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

Answer: A

NEW QUESTION 171

- (Topic 4)

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

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

Answer: C

NEW QUESTION 173

- (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 176

- (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 181

- (Topic 4)

The process of creating a system which divides documents based on their security level to manage access to private data is known as

- A. security coding
- B. data security system
- C. data classification
- D. privacy protection

Answer: C

NEW QUESTION 182

- (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 183

- (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 185

- (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 189

- (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 193

- (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 197

- (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 198

- (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 implemented remediation activities. Which of the following is the MOST logical next step?

- A. Validate the effectiveness of applied controls
- B. Validate security program resource requirements
- 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: A

NEW QUESTION 200

- (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 202

- (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 203

- (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 208

- (Topic 5)

What is the BEST reason for having a formal request for proposal process?

- A. Creates a timeline for purchasing and budgeting
- B. Allows small companies to compete with larger companies
- C. Clearly identifies risks and benefits before funding is spent
- D. Informs suppliers a company is going to make a purchase

Answer: C

NEW QUESTION 210

- (Topic 5)

As the CISO you need to write the IT security strategic plan. Which of the following is the MOST important to review before you start writing the plan?

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

Answer: B

NEW QUESTION 212

- (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 215

- (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 216

- (Topic 5)

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

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

Answer: C

NEW QUESTION 219

- (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 220

- (Topic 5)

The rate of change in technology increases the importance of:

- A. Outsourcing the IT functions.
- B. Understanding user requirements.
- C. Hiring personnel with leading edge skills.
- D. Implementing and enforcing good processes.

Answer: D

NEW QUESTION 224

- (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 228

- (Topic 5)

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

Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

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

Answer: A

NEW QUESTION 233

- (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 234

- (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 frameworks and standards will BEST fit the organization as a baseline for their security program?

- A. NIST and Privacy Regulations
- B. ISO 27000 and Payment Card Industry Data Security Standards
- C. NIST and data breach notification laws
- D. ISO 27000 and Human resources best practices

Answer: B

NEW QUESTION 239

- (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 240

- (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 244

- (Topic 5)

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

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

Answer: B

NEW QUESTION 249

- (Topic 5)

SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs.

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

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

Answer: B

NEW QUESTION 253

- (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. Recently, members of your organization have been targeted through a number of sophisticated phishing attempts and have compromised their system credentials. What action can you take to prevent the misuse of compromised credentials to change bank account information from outside your organization while still allowing employees to manage their bank information?

- A. Turn off VPN access for users originating from outside the country
- B. Enable monitoring on the VPN for suspicious activity
- C. Force a change of all passwords

D. Block access to the Employee-Self Service application via VPN

Answer: D

NEW QUESTION 255

- (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 260

- (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 264

- (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 267

- (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 271

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 712-50 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 712-50 Product From:

<https://www.2passeasy.com/dumps/712-50/>

Money Back Guarantee

712-50 Practice Exam Features:

- * 712-50 Questions and Answers Updated Frequently
- * 712-50 Practice Questions Verified by Expert Senior Certified Staff
- * 712-50 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 712-50 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year