

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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



NEW QUESTION 1

- (Topic 1)

One of the MAIN goals of a Business Continuity Plan is to

- A. Ensure all infrastructure and applications are available in the event of a disaster
- B. Allow all technical first-responders to understand their roles in the event of a disaster
- C. Provide step by step plans to recover business processes in the event of a disaster
- D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer: C

NEW QUESTION 2

- (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 3

- (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 4

- (Topic 1)

Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 5

- (Topic 1)

Risk is defined as:

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

Answer: A

NEW QUESTION 6

- (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 7

- (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 8

- (Topic 1)

When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

- A. An independent Governance, Risk and Compliance organization
- B. Alignment of security goals with business goals
- C. Compliance with local privacy regulations
- D. Support from Legal and HR teams

Answer: B

NEW QUESTION 9

- (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 10

- (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 10

- (Topic 1)

Which of the following is the MOST important for a CISO to understand when identifying threats?

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

Answer: A

NEW QUESTION 14

- (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 16

- (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 20

- (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 22

- (Topic 1)

Which of the following should be determined while defining risk management strategies?

- A. Organizational objectives and risk tolerance
- B. Risk assessment criteria
- C. IT architecture complexity
- D. Enterprise disaster recovery plans

Answer: A

NEW QUESTION 24

- (Topic 1)

Which of the following has the GREATEST impact on the implementation of an information security governance model?

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

Answer: D

NEW QUESTION 28

- (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 32

- (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 33

- (Topic 1)

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

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

Answer: A

NEW QUESTION 38

- (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 39

- (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 41

- (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 46

- (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 50

- (Topic 1)

The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

- A. Due Protection
- B. Due Care
- C. Due Compromise
- D. Due process

Answer: B

NEW QUESTION 53

- (Topic 1)

Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

- A. Reduction of budget
- B. Decreased security awareness
- C. Improper use of information resources
- D. Fines for regulatory non-compliance

Answer: D

NEW QUESTION 56

- (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 57

- (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 62

- (Topic 1)

Which of the following international standards can be BEST used to define a Risk Management process in an organization?

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

Answer: B

NEW QUESTION 65

- (Topic 1)

Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

- A. Audit and Legal
- B. Budget and Compliance
- C. Human Resources and Budget
- D. Legal and Human Resources

Answer: A

NEW QUESTION 70

- (Topic 2)

The regular review of a firewall ruleset is considered a

- A. Procedural control
- B. Organization control
- C. Technical control
- D. Management control

Answer: A

NEW QUESTION 74

- (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 78

- (Topic 2)

How often should an environment be monitored for cyber threats, risks, and exposures?

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

Answer: D

NEW QUESTION 79

- (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 83

- (Topic 2)

An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.

- A. Install software patch, Operate system, Maintain system
- B. Discover software, Remove affected software, Apply software patch
- C. Install software patch, configuration adjustment, Software Removal
- D. Software removal, install software patch, maintain system

Answer:

C

NEW QUESTION 86

- (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 87

- (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 89

- (Topic 2)

A missing/ineffective security control is identified. Which of the following should be the NEXT step?

- A. Perform an audit to measure the control formally
- B. Escalate the issue to the IT organization
- C. Perform a risk assessment to measure risk
- D. Establish Key Risk Indicators

Answer: C

NEW QUESTION 93

- (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 97

- (Topic 2)

IT control objectives are useful to IT auditors as they provide the basis for understanding the:

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

Answer: A

NEW QUESTION 102

- (Topic 2)

As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

- A. Executive summary
- B. Penetration test agreement
- C. Names and phone numbers of those who conducted the audit
- D. Business charter

Answer: A

NEW QUESTION 106

- (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 109

- (Topic 2)

When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

- A. Transfer financial resources from other critical programs
- B. Take the system off line until the budget is available
- C. Deploy countermeasures and compensating controls until the budget is available
- D. Schedule an emergency meeting and request the funding to fix the issue

Answer: C

NEW QUESTION 114

- (Topic 2)

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

- A. Qualitative analysis
- B. Quantitative analysis
- C. Risk mitigation
- D. Estimate activity duration

Answer: A

NEW QUESTION 115

- (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 117

- (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 119

- (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 122

- (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 126

- (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 128

- (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 130

- (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 133

- (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 137

- (Topic 2)

The patching and monitoring of systems on a consistent schedule is required by?

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

Answer: C

NEW QUESTION 142

- (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 144

- (Topic 3)

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

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

Answer: B

NEW QUESTION 147

- (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 151

- (Topic 3)

An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in severe revenue disruptions. Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

- A. The CISO
- B. Audit and Compliance
- C. The CFO
- D. The business owner

Answer: D

NEW QUESTION 153

- (Topic 3)

The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong? (choose the BEST answer):

- A. Failed to identify all stakeholders and their needs
- B. Deployed the encryption solution in an inadequate manner
- C. Used 1024 bit encryption when 256 bit would have sufficed
- D. Used hardware encryption instead of software encryption

Answer: A

NEW QUESTION 157

- (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 159

- (Topic 3)

Which of the following methodologies references the recommended industry standard that Information security project managers should follow?

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

Answer: D

NEW QUESTION 164

- (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 165

- (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 168

- (Topic 3)

A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:

- A. Change management
- B. Business continuity planning
- C. Security Incident Response
- D. Thought leadership

Answer: C

NEW QUESTION 170

- (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 173

- (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 174

- (Topic 3)

In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?

- A. Vmware, router, switch, firewall, syslog, vulnerability management system (VMS)
- B. Intrusion Detection System (IDS), firewall, switch, syslog
- C. Security Incident Event Management (SIEM), IDS, router, syslog
- D. SIEM, IDS, firewall, VMS

Answer: D

NEW QUESTION 179

- (Topic 3)

The organization does not have the time to remediate the vulnerability; however it is critical to release the application. Which of the following needs to be further evaluated to help mitigate the risks?

- A. Provide developer security training
- B. Deploy Intrusion Detection Systems
- C. Provide security testing tools
- D. Implement Compensating Controls

Answer: D

NEW QUESTION 184

- (Topic 3)

Which of the following is considered a project versus a managed process?

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

Answer: D

NEW QUESTION 187

- (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 188

- (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 190

- (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 194

- (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 199

- (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 203

- (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 205

- (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 210

- (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 214

- (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 217

- (Topic 3)

A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

- A. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
- B. A clear set of security policies and procedures that are more concept-based than controls-based
- C. A complete inventory of Information Technology assets including infrastructure, networks, applications and data
- D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

Answer: :D

NEW QUESTION 222

- (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 223

- (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 227

- (Topic 4)

You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

- A. Execute
- B. Read
- C. Administrator
- D. Public

Answer: D

NEW QUESTION 230

- (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 234

- (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 237

- (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 239

- (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 244

- (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 245

- (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 248

- (Topic 4)

Which of the following is a symmetric encryption algorithm?

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

Answer: A

NEW QUESTION 251

- (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 254

- (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 258

- (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 259

- (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 260

- (Topic 5)

What is the primary reason for performing a return on investment analysis?

- A. To decide between multiple vendors
- B. To decide is the solution costs less than the risk it is mitigating
- C. To determine the current present value of a project
- D. To determine the annual rate of loss

Answer: B

NEW QUESTION 263

- (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 266

- (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 270

- (Topic 5)

Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates. When multiple regulations or standards apply to your industry you should set controls to meet the:

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

Answer: A

NEW QUESTION 271

- (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 275

- (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 278

- (Topic 5)

When creating contractual agreements and procurement processes why should security requirements be included?

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

Answer: B

NEW QUESTION 282

- (Topic 5)

SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning. Which of the following is the MOST logical next step?

- A. Validate the effectiveness of current controls
- B. Create detailed remediation funding and staffing plans
- C. Report the audit findings and remediation status to business stake holders
- D. Review security procedures to determine if they need modified according to findings

Answer: C

NEW QUESTION 283

- (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 286

- (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 290

- (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 291

- (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 294

- (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 295

- (Topic 5)

Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:

- A. Create timelines for mitigation
- B. Develop a cost-benefit analysis
- C. Calculate annual loss expectancy
- D. Create a detailed technical executive summary

Answer: B

NEW QUESTION 296

- (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 299

- (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 304

- (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 306

- (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.”

What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

- A. Cite compliance with laws, statutes, and regulations – explaining the financial implications for the company for non-compliance
- B. Understand the business and focus your efforts on enabling operations securely
- C. Draw from your experience and recount stories of how other companies have been compromised
- D. Cite corporate policy and insist on compliance with audit findings

Answer: B

NEW QUESTION 311

- (Topic 5)

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

What action should you take FIRST?

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

Answer: C

NEW QUESTION 316

- (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-factor 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 320

- (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 323

- (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 324

- (Topic 5)

When dealing with risk, the information security practitioner may choose to:

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

Answer: C

NEW QUESTION 326

- (Topic 5)

Involvement of senior management is MOST important in the development of:

- A. IT security implementation plans.
- B. Standards and guidelines.
- C. IT security policies.
- D. IT security procedures.

Answer: C

NEW QUESTION 327

- (Topic 5)

The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

- A. Safeguard Value
- B. Cost Benefit Analysis
- C. Single Loss Expectancy
- D. Life Cycle Loss Expectancy

Answer: B

NEW QUESTION 332

- (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 334

- (Topic 5)

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

You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

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

Answer: :A

NEW QUESTION 338

- (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 340

- (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 344

.....

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