

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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



NEW QUESTION 1

- (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 2

- (Topic 1)

Credit card information, medical data, and government records are all examples of:

- A. Confidential/Protected Information
- B. Bodily Information
- C. Territorial Information
- D. Communications Information

Answer: A

NEW QUESTION 3

- (Topic 1)

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

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

Answer: C

NEW QUESTION 4

- (Topic 1)

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

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

Answer: D

NEW QUESTION 5

- (Topic 1)

According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

- A. Susceptibility to attack, mitigation response time, and cost
- B. Attack vectors, controls cost, and investigation staffing needs
- C. Vulnerability exploitation, attack recovery, and mean time to repair
- D. Susceptibility to attack, expected duration of attack, and mitigation availability

Answer: A

NEW QUESTION 6

- (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 7

- (Topic 1)

A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

- A. Enforce the existing security standards and do not allow the deployment of the new technology.
- B. Amend the standard to permit the deployment.

- C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
- D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Answer: C

NEW QUESTION 8

- (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 9

- (Topic 1)

Payment Card Industry (PCI) compliance requirements are based on what criteria?

- A. The types of cardholder data retained
- B. The duration card holder data is retained
- C. The size of the organization processing credit card data
- D. The number of transactions performed per year by an organization

Answer: D

NEW QUESTION 10

- (Topic 1)

From an information security perspective, information that no longer supports the main purpose of the business should be:

- A. assessed by a business impact analysis.
- B. protected under the information classification policy.
- C. analyzed under the data ownership policy.
- D. analyzed under the retention policy

Answer: D

NEW QUESTION 10

- (Topic 1)

What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

- A. Determine appetite
- B. Evaluate risk avoidance criteria
- C. Perform a risk assessment
- D. Mitigate risk

Answer: D

NEW QUESTION 11

- (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 16

- (Topic 1)

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

- A. When there is a need to develop a more unified incident response capability.
- B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
- C. When there is a variety of technologies deployed in the infrastructure.
- D. When it results in an overall lower cost of operating the security program.

Answer: B

NEW QUESTION 18

- (Topic 1)

The Information Security Governance program MUST:

- A. integrate with other organizational governance processes
- B. support user choice for Bring Your Own Device (BYOD)
- C. integrate with other organizational governance processes
- D. show a return on investment for the organization

Answer: A

NEW QUESTION 21

- (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 23

- (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 25

- (Topic 1)

Risk appetite directly affects what part of a vulnerability management program?

- A. Staff
- B. Scope
- C. Schedule
- D. Scan tools

Answer: B

NEW QUESTION 29

- (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 31

- (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 32

- (Topic 1)

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

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

Answer: C

NEW QUESTION 36

- (Topic 1)

Developing effective security controls is a balance between:

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

Answer: A

NEW QUESTION 39

- (Topic 1)

What is the main purpose of the Incident Response Team?

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

Answer: A

NEW QUESTION 41

- (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 44

- (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 46

- (Topic 1)

The single most important consideration to make when developing your security program, policies, and processes is:

- A. Budgeting for unforeseen data compromises
- B. Streamlining for efficiency
- C. Alignment with the business
- D. Establishing your authority as the Security Executive

Answer: C

NEW QUESTION 47

- (Topic 1)

Who is responsible for securing networks during a security incident?

- A. Chief Information Security Officer (CISO)
- B. Security Operations Center (SOC)
- C. Disaster Recovery (DR) manager
- D. Incident Response Team (IRT)

Answer: D

NEW QUESTION 49

- (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 54

- (Topic 1)

The PRIMARY objective of security awareness is to:

- A. Ensure that security policies are read.
- B. Encourage security-conscious employee behavior.
- C. Meet legal and regulatory requirements.
- D. Put employees on notice in case follow-up action for noncompliance is necessary

Answer: B

NEW QUESTION 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 61

- (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 65

- (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 67

- (Topic 2)

At which point should the identity access management team be notified of the termination of an employee?

- A. At the end of the day once the employee is off site
- B. During the monthly review cycle
- C. Immediately so the employee account(s) can be disabled
- D. Before an audit

Answer: C

NEW QUESTION 71

- (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 75

- (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 80

- (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 82

- (Topic 2)

Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

- A. Use within an organization to formulate security requirements and objectives
- B. Implementation of business-enabling information security
- C. Use within an organization to ensure compliance with laws and regulations
- D. To enable organizations that adopt it to obtain certifications

Answer: B

NEW QUESTION 87

- (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 89

- (Topic 2)

Which of the following is the MOST important goal of risk management?

- A. Identifying the risk
- B. Finding economic balance between the impact of the risk and the cost of the control
- C. Identifying the victim of any potential exploits.
- D. Assessing the impact of potential threats

Answer: B

NEW QUESTION 92

- (Topic 2)

Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

- A. Single Loss Expectancy (SLE)
- B. Exposure Factor (EF)
- C. Annualized Rate of Occurrence (ARO)
- D. Temporal Probability (TP)

Answer: C

NEW QUESTION 95

- (Topic 2)

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

- A. Plan-Check-Do-Act
- B. Plan-Do-Check-Act
- C. Plan-Select-Implement-Evaluate
- D. SCORE (Security Consensus Operational Readiness Evaluation)

Answer: B

NEW QUESTION 97

- (Topic 2)

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

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

Answer: C

NEW QUESTION 98

- (Topic 2)

Dataflow diagrams are used by IT auditors to:

- A. Order data hierarchically.
- B. Highlight high-level data definitions.
- C. Graphically summarize data paths and storage processes.
- D. Portray step-by-step details of data generation.

Answer: C

NEW QUESTION 99

- (Topic 2)

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 102

- (Topic 2)

An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:

- A. Inform senior management of the risk involved.
- B. Agree to work with the security officer on these shifts as a form of preventative control.
- C. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
- D. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.

Answer: A

NEW QUESTION 105

- (Topic 2)

Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

- A. Servers, routers, switches, modem
- B. Firewall, exchange, web server, intrusion detection system (IDS)
- C. Firewall, anti-virus console, IDS, syslog
- D. IDS, syslog, router, switches

Answer: C

NEW QUESTION 110

- (Topic 2)

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

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

Answer: C

NEW QUESTION 112

- (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 114

- (Topic 2)

To have accurate and effective information security policies how often should the CISO review the organization policies?

- A. Every 6 months
- B. Quarterly
- C. Before an audit
- D. At least once a year

Answer: D

NEW QUESTION 117

- (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 121

- (Topic 2)

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

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

Answer: A

NEW QUESTION 124

- (Topic 2)

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

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

Answer: C

NEW QUESTION 126

- (Topic 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 127

- (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 129

- (Topic 3)

A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability. What do you do?

- A. tell him to shut down the server
- B. tell him to call the police
- C. tell him to invoke the incident response process
- D. tell him to analyze the problem, preserve the evidence and provide a full analysis and report

Answer: C

NEW QUESTION 134

- (Topic 3)

Which of the following are not stakeholders of IT security projects?

- A. Board of directors
- B. Third party vendors
- C. CISO
- D. Help Desk

Answer: B

NEW QUESTION 139

- (Topic 3)

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

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

Answer: C

NEW QUESTION 144

- (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 149

- (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 153

- (Topic 3)

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

- A. Vendors uses their own laptop and logins with same admin credentials your security team uses
- B. Vendor uses a company supplied laptop and logins using two factor authentication with same admin credentials your security team uses
- C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials
- D. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials

Answer: C

NEW QUESTION 154

- (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 159

- (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 163

- (Topic 3)

How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?

- A. Quarterly
- B. Semi-annually
- C. Bi-annually
- D. Annually

Answer: D

NEW QUESTION 165

- (Topic 3)

As the CISO for your company you are accountable for the protection of information resources commensurate with:

- A. Customer demand
- B. Cost and time to replace
- C. Insurability tables
- D. Risk of exposure

Answer: D

NEW QUESTION 168

- (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 173

- (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 176

- (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 179

- (Topic 4)

An anonymity network is a series of?

- A. Covert government networks
- B. War driving maps
- C. Government networks in Tora

D. Virtual network tunnels

Answer: D

NEW QUESTION 183

- (Topic 4)

An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

- A. Shared key
- B. Asynchronous
- C. Open
- D. None

Answer: A

NEW QUESTION 186

- (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 190

- (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 195

- (Topic 4)

Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?

- A. In-line hardware keyloggers don't require physical access
- B. In-line hardware keyloggers don't comply to industry regulations
- C. In-line hardware keyloggers are undetectable by software
- D. In-line hardware keyloggers are relatively inexpensive

Answer: C

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 201

- (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 205

- (Topic 5)

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

Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time. Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

- A. Security Guards posted outside the Data Center
- B. Data Loss Prevention (DLP)
- C. Rigorous syslog reviews
- D. Intrusion Detection Systems (IDS)

Answer: B

NEW QUESTION 210

- (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 212

- (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 216

- (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 217

- (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 221

- (Topic 5)

Annual Loss Expectancy is derived from the function of which two factors?

- A. Annual Rate of Occurrence and Asset Value
- B. Single Loss Expectancy and Exposure Factor
- C. Safeguard Value and Annual Rate of Occurrence
- D. Annual Rate of Occurrence and Single Loss Expectancy

Answer: D

NEW QUESTION 223

- (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 226

- (Topic 5)

John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can John do in this instance?

- A. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
- B. Review the Request for Proposal (RFP) for guidance.
- C. Withhold the vendor's payments until the issue is resolved.
- D. Refer to the contract agreement for direction.

Answer: D

NEW QUESTION 230

- (Topic 5)

Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers."
Which group of people should be consulted when developing your security program?

- A. Peers
- B. End Users
- C. Executive Management
- D. All of the above

Answer: :D

NEW QUESTION 234

- (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 238

- (Topic 5)

The total cost of security controls should:

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

Answer: C

NEW QUESTION 241

- (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 244

- (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 245

- (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. What is the MOST logical course of action the CISO should take?

- A. Review the original solution set to determine if another system would fit the organization's risk appetite and budget regulatory compliance requirements
- B. Continue with the implementation and submit change requests to the vendor in order to ensure required functionality will be provided when needed
- C. Continue with the project until the scalability issue is validated by others, such as an auditor or third party assessor
- D. Cancel the project if the business need was based on internal requirements versus regulatory compliance requirements

Answer: A

NEW QUESTION 250

- (Topic 5)

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

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

Answer: C

NEW QUESTION 255

- (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 258

- (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 261

- (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 265

.....

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