



EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

NEW QUESTION 1

- (Topic 1)

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

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

Answer: A

NEW QUESTION 2

- (Topic 1)

Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 3

- (Topic 1)

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

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

Answer: D

NEW QUESTION 4

- (Topic 1)

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 5

- (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 6

- (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 7

- (Topic 1)

Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

- A. Awareness
- B. Compliance

- C. Governance
- D. Management

Answer: C

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 dealing with a risk management process, asset classification is important because it will impact the overall:

- A. Threat identification
- B. Risk monitoring
- C. Risk treatment
- D. Risk tolerance

Answer: C

NEW QUESTION 10

- (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)

In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

- A. High risk environments 6 months, low risk environments 12 months
- B. Every 12 months
- C. Every 18 months
- D. Every six months

Answer: B

NEW QUESTION 12

- (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 17

- (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 22

- (Topic 1)

Who in the organization determines access to information?

- A. Legal department
- B. Compliance officer
- C. Data Owner
- D. Information security officer

Answer: C

NEW QUESTION 23

- (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 26

- (Topic 1)

What is a difference from the list below between quantitative and qualitative Risk Assessment?

- A. Quantitative risk assessments result in an exact number (in monetary terms)
- B. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
- C. Qualitative risk assessments map to business objectives
- D. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Answer: A

NEW QUESTION 29

- (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 32

- (Topic 1)

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

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

Answer: C

NEW QUESTION 33

- (Topic 1)

A method to transfer risk is to:

- A. Implement redundancy
- B. move operations to another region
- C. purchase breach insurance
- D. Alignment with business operations

Answer: C

NEW QUESTION 35

- (Topic 1)

The FIRST step in establishing a security governance program is to?

- A. Conduct a risk assessment.
- B. Obtain senior level sponsorship.
- C. Conduct a workshop for all end users.
- D. Prepare a security budget.

Answer: :B

NEW QUESTION 36

- (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 39

- (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 44

- (Topic 1)

When briefing senior management on the creation of a governance process, the MOST important aspect should be:

- A. information security metrics.
- B. knowledge required to analyze each issue.
- C. baseline against which metrics are evaluated.
- D. linkage to business area objectives.

Answer: D

NEW QUESTION 49

- (Topic 1)

Why is it vitally important that senior management endorse a security policy?

- A. So that they will accept ownership for security within the organization.
- B. So that employees will follow the policy directives.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they can be held legally accountable.

Answer: A

NEW QUESTION 52

- (Topic 1)

The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for

- A. Confidentiality, Integrity and Availability
- B. Assurance, Compliance and Availability
- C. International Compliance
- D. Integrity and Availability

Answer: A

NEW QUESTION 57

- (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 60

- (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 63

- (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 66

- (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 71

- (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 75

- (Topic 1)

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

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

Answer: B

NEW QUESTION 80

- (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 81

- (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 82

- (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 86

- (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 90

- (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 92

- (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 93

- (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 94

- (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 99

- (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 101

- (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 105

- (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 109

- (Topic 1)

Risk that remains after risk mitigation is known as

- A. Persistent risk
- B. Residual risk
- C. Accepted risk
- D. Non-tolerated risk

Answer: B

NEW QUESTION 112

- (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 114

- (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 116

- (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 117

- (Topic 2)

When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

- A. Threat Level, Risk of Compromise, and Consequences of Compromise
- B. Risk Avoidance, Threat Level, and Consequences of Compromise
- C. Risk Transfer, Reputational Impact, and Consequences of Compromise
- D. Reputational Impact, Financial Impact, and Risk of Compromise

Answer: A

NEW QUESTION 119

- (Topic 2)

An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

- A. Management Control
- B. Technical Control
- C. Training Control
- D. Operational Control

Answer: D

NEW QUESTION 124

- (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 125

- (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 128

- (Topic 2)

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

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

Answer: A

NEW QUESTION 131

- (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 135

- (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 137

- (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 140

- (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 142

- (Topic 2)

Creating a secondary authentication process for network access would be an example of?

- A. Nonlinearities in physical security performance metrics
- B. Defense in depth cost enumerated costs
- C. System hardening and patching requirements
- D. Anti-virus for mobile devices

Answer: A

NEW QUESTION 146

- (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 150

- (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 151

- (Topic 2)

Which of the following illustrates an operational control process:

- A. Classifying an information system as part of a risk assessment
- B. Installing an appropriate fire suppression system in the data center
- C. Conducting an audit of the configuration management process
- D. Establishing procurement standards for cloud vendors

Answer: :B

NEW QUESTION 155

- (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 157

- (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 162

- (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 167

- (Topic 2)

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

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

Answer: B

NEW QUESTION 169

- (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 173

- (Topic 2)

Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

- A. ISO 27001
- B. ISO 27002
- C. ISO 27004
- D. ISO 27005

Answer: :D

NEW QUESTION 174

- (Topic 2)

Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?

- A. All vulnerabilities found on servers and desktops
- B. Only critical and high vulnerabilities on servers and desktops
- C. Only critical and high vulnerabilities that impact important production servers
- D. All vulnerabilities that impact important production servers

Answer: C

NEW QUESTION 177

- (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 181

- (Topic 2)

Creating a secondary authentication process for network access would be an example of?

- A. An administrator with too much time on their hands.
- B. Putting undue time commitment on the system administrator.
- C. Supporting the concept of layered security
- D. Network segmentation.

Answer: C

NEW QUESTION 183

- (Topic 2)

Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

- A. International Organization for Standardization 27001
- B. National Institute of Standards and Technology Special Publication SP 800-12
- C. Request For Comment 2196
- D. National Institute of Standards and Technology Special Publication SP 800-26

Answer: A

NEW QUESTION 185

- (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 187

- (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 189

- (Topic 2)

With respect to the audit management process, management response serves what function?

- A. placing underperforming units on notice for failing to meet standards
- B. determining whether or not resources will be allocated to remediate a finding
- C. adding controls to ensure that proper oversight is achieved by management
- D. revealing the “root cause” of the process failure and mitigating for all internal and external units

Answer: B

NEW QUESTION 190

- (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 194

- (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 199

- (Topic 2)

The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization's

- A. Risk Management Program.
- B. Anti-Spam controls.
- C. Security Awareness Program.
- D. Identity and Access Management Program.

Answer: C

NEW QUESTION 200

- (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 205

- (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 208

- (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 210

- (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 211

- (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 213

- (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 214

- (Topic 2)

The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

- A. The asset is more expensive than the remediation
- B. The audit finding is incorrect
- C. The asset being protected is less valuable than the remediation costs
- D. The remediation costs are irrelevant; it must be implemented regardless of cost.

Answer: C

NEW QUESTION 215

- (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 220

- (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 225

- (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 228

- (Topic 3)

Which of the following information may be found in table top exercises for incident response?

- A. Security budget augmentation
- B. Process improvements
- C. Real-time to remediate
- D. Security control selection

Answer: B

NEW QUESTION 233

- (Topic 3)

When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

- A. Type of data contained in the process/system
- B. Type of connection/protocol used to transfer the data
- C. Type of encryption required for the data once it is at rest
- D. Type of computer the data is processed on

Answer: A

NEW QUESTION 234

- (Topic 3)

A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?

- A. Poor audit support for the security program
- B. A lack of executive presence within the security program
- C. Poor alignment of the security program to business needs
- D. This is normal since business units typically resist security requirements

Answer: C

NEW QUESTION 235

- (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 238

- (Topic 3)

Which business stakeholder is accountable for the integrity of a new information system?

- A. CISO
- B. Compliance Officer
- C. Project manager
- D. Board of directors

Answer: A

NEW QUESTION 243

- (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 247

- (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 248

- (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 252

- (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 257

- (Topic 3)

Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

- A. Security administrators
- B. Security managers
- C. Security technicians
- D. Security analysts

Answer: B

NEW QUESTION 260

- (Topic 3)

The ultimate goal of an IT security projects is:

- A. Increase stock value
- B. Complete security
- C. Support business requirements
- D. Implement information security policies

Answer: C

NEW QUESTION 261

- (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 262

- (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 264

- (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 266

- (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 270

- (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 271

- (Topic 3)

This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

- A. Scope creep
- B. Deadline extension
- C. Scope modification
- D. Deliverable expansion

Answer: A

NEW QUESTION 273

- (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 278

- (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 282

- (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 284

- (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 285

- (Topic 3)

Which of the following is a major benefit of applying risk levels?

- A. Risk management governance becomes easier since most risks remain low once mitigated
- B. Resources are not wasted on risks that are already managed to an acceptable level
- C. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology
- D. Risk appetite can increase within the organization once the levels are understood

Answer: B

NEW QUESTION 286

- (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 291

- (Topic 3)

Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

- A. Define the risk appetite
- B. Determine budget constraints
- C. Review project charters
- D. Collaborate security projects

Answer: A

NEW QUESTION 292

- (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 296

- (Topic 3)

Which of the following can the company implement in order to avoid this type of security issue in the future?

- A. Network based intrusion detection systems
- B. A security training program for developers
- C. A risk management process
- D. A audit management process

Answer: B

NEW QUESTION 300

- (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 301

- (Topic 3)

A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?

- A. The software license expiration is probably out of synchronization with other software licenses
- B. The project was initiated without an effort to get support from impacted business units in the organization
- C. The software is out of date and does not provide for a scalable solution across the enterprise
- D. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects

Answer: B

NEW QUESTION 304

- (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 308

- (Topic 3)

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 312

- (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 315

- (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 317

- (Topic 3)

You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do. What is the BEST approach to handle this situation?

- A. Tell the team to do their best and respond to each alert
- B. Tune the sensors to help reduce false positives so the team can react better
- C. Request additional resources to handle the workload
- D. Tell the team to only respond to the critical and high alerts

Answer: B

NEW QUESTION 318

- (Topic 3)

A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets. This demonstrates which of the following principles?

- A. Security alignment to business goals
- B. Regulatory compliance effectiveness
- C. Increased security program presence
- D. Proper organizational policy enforcement

Answer: A

NEW QUESTION 322

- (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 325

- (Topic 3)

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

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

Answer: C

NEW QUESTION 330

- (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 334

- (Topic 4)

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

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

Answer: :C

NEW QUESTION 339

- (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 344

- (Topic 4)

Which of the following is the MAIN security concern for public cloud computing?

- A. Unable to control physical access to the servers
- B. Unable to track log on activity
- C. Unable to run anti-virus scans
- D. Unable to patch systems as needed

Answer: A

NEW QUESTION 349

- (Topic 4)

Which wireless encryption technology makes use of temporal keys?

- A. Wireless Application Protocol (WAP)
- B. Wifi Protected Access version 2 (WPA2)
- C. Wireless Equivalence Protocol (WEP)
- D. Extensible Authentication Protocol (EAP)

Answer: B

NEW QUESTION 351

- (Topic 4)

In terms of supporting a forensic investigation, it is now imperative that managers, first- responders, etc., accomplish the following actions to the computer under investigation:

- A. Secure the area and shut-down the computer until investigators arrive
- B. Secure the area and attempt to maintain power until investigators arrive
- C. Immediately place hard drive and other components in an anti-static bag
- D. Secure the area.

Answer: B

NEW QUESTION 356

- (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 357

- (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 360

- (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 362

- (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 366

- (Topic 4)

SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 370

- (Topic 4)

A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?

- A. non-repudiation
- B. conflict resolution
- C. strong authentication
- D. digital rights management

Answer: A

NEW QUESTION 373

- (Topic 4)

Security related breaches are assessed and contained through which of the following?

- A. The IT support team.
- B. A forensic analysis.
- C. Incident response
- D. Physical security team.

Answer:

C

NEW QUESTION 377

- (Topic 4)

Which of the following is a symmetric encryption algorithm?

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

Answer: A

NEW QUESTION 382

- (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 385

- (Topic 4)

Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

- A. Trusted and untrusted networks
- B. Type of authentication
- C. Storage encryption
- D. Log retention

Answer: A

NEW QUESTION 386

- (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 389

- (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. What type of control is being implemented by supervisors and data owners?

- A. Management
- B. Operational
- C. Technical
- D. Administrative

Answer: B

NEW QUESTION 390

- (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 394

- (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 395

- (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 398

- (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 400

- (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.

During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical aspect of the team's activities?

- A. Regular communication of incident status to executives
- B. Eradication of malware and system restoration
- C. Determination of the attack source
- D. Preservation of information

Answer: D

NEW QUESTION 405

- (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.

From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?

- A. Lack of risk management process
- B. Lack of sponsorship from executive management
- C. IT security centric agenda
- D. Compliance centric agenda

Answer: C

NEW QUESTION 408

- (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 410

- (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 414

- (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 419

- (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 423

- (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 426

- (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 428

- (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 433

- (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 437

- (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 440

- (Topic 5)

The formal certification and accreditation process has four primary steps, what are they?

- A. Evaluating, describing, testing and authorizing
- B. Evaluating, purchasing, testing, authorizing
- C. Auditing, documenting, verifying, certifying
- D. Discovery, testing, authorizing, certifying

Answer: A

NEW QUESTION 441

- (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 446

- (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 447

- (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 451

- (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 453

- (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 458

- (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 459

- (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 462

- (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 467

- (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 472

- (Topic 5)

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

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

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

Answer: A

NEW QUESTION 474

- (Topic 5)

Which of the following is MOST useful when developing a business case for security initiatives?

- A. Budget forecasts
- B. Request for proposals
- C. Cost/benefit analysis
- D. Vendor management

Answer: C

NEW QUESTION 479

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The 712-50 Practice Test Here](#)