

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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



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)

Regulatory requirements typically force organizations to implement

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

Answer: A

NEW QUESTION 3

- (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 4

- (Topic 1)

Which of the following are the MOST important factors for proactively determining system vulnerabilities?

- A. Subscribe to vendor mailing list to get notification of system vulnerabilities
- B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
- C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
- D. Conduct security testing, vulnerability scanning, and penetration testing

Answer: D

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (Topic 1)

The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

- A. Contacting the Internet Service Provider for an IP scope
- B. Getting authority to operate the system from executive management
- C. Changing the default passwords
- D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

NEW QUESTION 9

- (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 10

- (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 14

- (Topic 1)

If your organization operates under a model of "assumption of breach", you should:

- A. Protect all information resource assets equally
- B. Establish active firewall monitoring protocols
- C. Purchase insurance for your compliance liability
- D. Focus your security efforts on high value assets

Answer: :C

NEW QUESTION 16

- (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 20

- (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 22

- (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 25

- (Topic 1)

Which of the following is considered the MOST effective tool against social engineering?

- A. Anti-phishing tools
- B. Anti-malware tools
- C. Effective Security Vulnerability Management Program
- D. Effective Security awareness program

Answer: D

NEW QUESTION 30

- (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 31

- (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 34

- (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 36

- (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 37

- (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 38

- (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 41

- (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 46

- (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 50

- (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 54

- (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 59

- (Topic 1)

Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

- A. Strong authentication technologies
- B. Financial reporting regulations
- C. Credit card compliance and regulations
- D. Local privacy laws

Answer: D

NEW QUESTION 61

- (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 63

- (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 67

- (Topic 1)

The alerting, monitoring and life-cycle management of security related events is typically handled by the

- A. security threat and vulnerability management process
- B. risk assessment process
- C. risk management process
- D. governance, risk, and compliance tools

Answer: :A

NEW QUESTION 69

- (Topic 1)

When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

- A. How many credit card records are stored?
- B. How many servers do you have?
- C. What is the scope of the certification?
- D. What is the value of the assets at risk?

Answer: C

NEW QUESTION 74

- (Topic 1)

According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

- A. Identify threats, risks, impacts and vulnerabilities
- B. Decide how to manage risk
- C. Define the budget of the Information Security Management System
- D. Define Information Security Policy

Answer: D

NEW QUESTION 76

- (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 77

- (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 81

- (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 86

- (Topic 1)

When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

- A. Escalation
- B. Recovery
- C. Eradication
- D. Containment

Answer: D

NEW QUESTION 89

- (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 94

- (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 96

- (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 100

- (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 102

- (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 105

- (Topic 1)

The Information Security Management program MUST protect:

- A. all organizational assets
- B. critical business processes and /or revenue streams
- C. intellectual property released into the public domain
- D. against distributed denial of service attacks

Answer: B

NEW QUESTION 108

- (Topic 1)

A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

- A. Compliance to the Payment Card Industry (PCI) regulations.
- B. Alignment with financial reporting regulations for each country where they operate.
- C. Alignment with International Organization for Standardization (ISO) standards.
- D. Compliance with patient data protection regulations for each country where they operate.

Answer: D

NEW QUESTION 113

- (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 118

- (Topic 1)

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

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

Answer: B

NEW QUESTION 120

- (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 121

- (Topic 1)

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

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

Answer: B

NEW QUESTION 125

- (Topic 1)

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

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

Answer: A

NEW QUESTION 127

- (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 128

- (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 129

- (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 134

- (Topic 2)

A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

- A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
- B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
- C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
- D. If the findings do not impact regulatory compliance, review current security controls.

Answer: C

NEW QUESTION 136

- (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 139

- (Topic 2)

Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

- A. Application logs
- B. File integrity monitoring
- C. SNMP traps

D. Syslog

Answer: B

NEW QUESTION 143

- (Topic 2)

Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

- A. To give information security management recommendations to those who are responsible for initiating, implementing, or maintaining security in their organization.
- B. To provide a common basis for developing organizational security standards
- C. To provide effective security management practice and to provide confidence in inter- organizational dealings
- D. To established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization

Answer: D

NEW QUESTION 145

- (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 148

- (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 150

- (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 155

- (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 157

- (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 159

- (Topic 2)

When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric

framework?

- A. ISO 27001
- B. PRINCE2
- C. ISO 27004
- D. ITILv3

Answer: C

NEW QUESTION 161

- (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 164

- (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 165

- (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 170

- (Topic 2)

The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is consider a bad practice MAINLY because

- A. The IT team is not familiar in IT audit practices
- B. This represents a bad implementation of the Least Privilege principle
- C. This represents a conflict of interest
- D. The IT team is not certified to perform audits

Answer: C

NEW QUESTION 173

- (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 176

- (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 180

- (Topic 2)

When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

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

Answer: A

NEW QUESTION 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 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 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 194

- (Topic 2)

A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?

- A. Have internal audit conduct another audit to see what has changed.
- B. Contract with an external audit company to conduct an unbiased audit
- C. Review the recommendations and follow up to see if audit implemented the changes
- D. Meet with audit team to determine a timeline for corrections

Answer: C

NEW QUESTION 199

- (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 203

- (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 208

- (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 210

- (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)

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 215

- (Topic 2)

The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

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

Answer: D

NEW QUESTION 217

- (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 218

- (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 221

- (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 226

- (Topic 3)

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

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

Answer: C

NEW QUESTION 227

- (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 231

- (Topic 3)

Your incident response plan should include which of the following?

- A. Procedures for litigation
- B. Procedures for reclamation
- C. Procedures for classification
- D. Procedures for charge-back

Answer: C

NEW QUESTION 234

- (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 235

- (Topic 3)

A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims. Which of the following vendor provided documents is BEST to make your decision:

- A. Vendor's client list of reputable organizations currently using their solution
- B. Vendor provided attestation of the detailed security controls from a reputable accounting firm
- C. Vendor provided reference from an existing reputable client detailing their implementation
- D. Vendor provided internal risk assessment and security control documentation

Answer: B

NEW QUESTION 240

- (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)

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 245

- (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 248

- (Topic 3)

Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed. What can be done to ensure that security is addressed cost effectively?

- A. User awareness training for all employees
- B. Installation of new firewalls and intrusion detection systems
- C. Launch an internal awareness campaign
- D. Integrate security requirements into project inception

Answer: D

NEW QUESTION 249

- (Topic 3)

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

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

Answer: D

NEW QUESTION 252

- (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 254

- (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 258

- (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 260

- (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 261

- (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 264

- (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 268

- (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 270

- (Topic 3)

An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents. Which of the following would be considered a MAJOR constraint for the project?

- A. Time zone differences
- B. Compliance to local hiring laws
- C. Encryption import/export regulations
- D. Local customer privacy laws

Answer: C

NEW QUESTION 272

- (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 277

- (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 278

- (Topic 3)

Which of the following represents the BEST method of ensuring security program alignment to business needs?

- A. Create a comprehensive security awareness program and provide success metrics to business units
- B. Create security consortiums, such as strategic security planning groups, that include business unit participation
- C. Ensure security implementations include business unit testing and functional validation prior to production rollout
- D. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role

Answer: B

NEW QUESTION 279

- (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 281

- (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 284

- (Topic 3)

What oversight should the information security team have in the change management process for application security?

- A. Information security should be informed of changes to applications only
- B. Development team should tell the information security team about any application security flaws
- C. Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production
- D. Information security should be aware of all application changes and work with developers before changes are deployed in production

Answer: C

NEW QUESTION 286

- (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 287

- (Topic 3)

When is an application security development project complete?

- A. When the application is retired.
- B. When the application turned over to production.
- C. When the application reaches the maintenance phase.

D. After one year.

Answer: A

NEW QUESTION 288

- (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 293

- (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 294

- (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 299

- (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 300

- (Topic 4)

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

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

Answer: C

NEW QUESTION 301

- (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 305

- (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 307

- (Topic 4)

The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?

- A. Well established and defined digital forensics process
- B. Establishing Enterprise-owned Botnets for preemptive attacks
- C. Be able to retaliate under the framework of Active Defense
- D. Collaboration with law enforcement

Answer: A

NEW QUESTION 312

- (Topic 4)

The general ledger setup function in an enterprise resource package allows for setting accounting periods. Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

- A. The need to change accounting periods on a regular basis.
- B. The requirement to post entries for a closed accounting period.
- C. The need to create and modify the chart of accounts and its allocations.
- D. The lack of policies and procedures for the proper segregation of duties.

Answer: D

NEW QUESTION 313

- (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 318

- (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 321

- (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 324

- (Topic 4)

What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

- A. Traffic Analysis
- B. Deep-Packet inspection
- C. Packet sampling
- D. Heuristic analysis

Answer: B

NEW QUESTION 328

- (Topic 4)

The process for identifying, collecting, and producing digital information in support of legal proceedings is called

- A. chain of custody.
- B. electronic discovery.
- C. evidence tampering.
- D. electronic review.

Answer: B

NEW QUESTION 332

- (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 336

- (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 339

- (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 340

- (Topic 4)

What is the FIRST step in developing the vulnerability management program?

- A. Baseline the Environment
- B. Maintain and Monitor
- C. Organization Vulnerability
- D. Define Policy

Answer: A

NEW QUESTION 345

- (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 349

- (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.

Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?

- A. Lack of identification of technology stake holders
- B. Lack of business continuity process
- C. Lack of influence with leaders outside IT

D. Lack of a security awareness program

Answer: C

NEW QUESTION 350

- (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 351

- (Topic 5)

The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called

- A. Security certification
- B. Security system analysis
- C. Security accreditation
- D. Alignment with business practices and goals.

Answer: A

NEW QUESTION 353

- (Topic 5)

Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.

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

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

Answer: B

NEW QUESTION 355

- (Topic 5)

The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

- A. Security certification
- B. Security system analysis
- C. Security accreditation
- D. Alignment with business practices and goals.

Answer: C

NEW QUESTION 358

- (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 362

- (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. Your Corporate Information Security Policy should include which of the following?

- A. Information security theory
- B. Roles and responsibilities
- C. Incident response contacts
- D. Desktop configuration standards

Answer: B

NEW QUESTION 364

- (Topic 5)

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

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

Answer: B

NEW QUESTION 366

- (Topic 5)

Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.

To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

- A. Business Impact Analysis
- B. Business Continuity plan
- C. Security roadmap
- D. Annual report to shareholders

Answer: A

NEW QUESTION 369

- (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 371

- (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 372

- (Topic 5)

Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.

When formulating the remediation plan, what is a required input?

- A. Board of directors
- B. Risk assessment
- C. Patching history
- D. Latest virus definitions file

Answer: B

NEW QUESTION 373

- (Topic 5)

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has

proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
How can you reduce the administrative burden of distributing symmetric keys for your employer?

- A. Use asymmetric encryption for the automated distribution of the symmetric key
- B. Use a self-generated key on both ends to eliminate the need for distribution
- C. Use certificate authority to distribute private keys
- D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

Answer: A

NEW QUESTION 374

- (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. The organization has already been subject to a significant amount of credit card fraud. Which of the following is the MOST likely reason for this fraud?

- A. Lack of compliance to the Payment Card Industry (PCI) standards
- B. Ineffective security awareness program
- C. Security practices not in alignment with ISO 27000 frameworks
- D. Lack of technical controls when dealing with credit card data

Answer: A

NEW QUESTION 377

- (Topic 5)

When analyzing and forecasting an operating expense budget what are not included?

- A. Software and hardware license fees
- B. Utilities and power costs
- C. Network connectivity costs
- D. New datacenter to operate from

Answer: D

NEW QUESTION 380

- (Topic 5)

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

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

Answer: B

NEW QUESTION 384

- (Topic 5)

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

- A. The Net Present Value (NPV) of the project is positive
- B. The NPV of the project is negative
- C. The Return on Investment (ROI) is larger than 10 months
- D. The ROI is lower than 10 months

Answer: B

NEW QUESTION 389

- (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 393

- (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 398

- (Topic 5)

Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the “real workers.”

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

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

Answer: B

NEW QUESTION 403

- (Topic 5)

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

Which of the following is the FIRST action the CISO will perform after receiving the audit report?

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

Answer: B

NEW QUESTION 405

- (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 406

- (Topic 5)

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

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

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

Answer: B

NEW QUESTION 408

- (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 413

- (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 414

- (Topic 5)

File Integrity Monitoring (FIM) is considered a

- A. Network based security preventative control
- B. Software segmentation control
- C. Security detective control
- D. User segmentation control

Answer: C

NEW QUESTION 417

- (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 422

- (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 424

- (Topic 5)

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

After determining the audit findings are accurate, which of the following is the MOST logical next activity?

- A. Begin initial gap remediation analyses
- B. Review the security organization's charter
- C. Validate gaps with the Information Technology team
- D. Create a briefing of the findings for executive management

Answer: A

NEW QUESTION 425

.....

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