

# EC-Council

## Exam Questions 712-50

EC-Council Certified CISO (CCISO)



#### NEW QUESTION 1

- (Exam Topic 6)

An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO).

The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?

- A. ISO 22318 Supply Chain Continuity
- B. ISO 27031 BCM Readiness
- C. ISO 22301 BCM Requirements
- D. ISO 22317 BIA

**Answer:** C

#### **Explanation:**

Reference: <https://www.smartsheet.com/content/iso-22301-business-continuity-guide>

#### NEW QUESTION 2

- (Exam Topic 6)

An auditor is reviewing the security classifications for a group of assets and finds that many of the assets are not correctly classified.

What should the auditor's NEXT step be?

- A. Immediately notify the board of directors of the organization as to the finding
- B. Correct the classifications immediately based on the auditor's knowledge of the proper classification
- C. Document the missing classifications
- D. Identify the owner of the asset and induce the owner to apply a proper classification

**Answer:** C

#### NEW QUESTION 3

- (Exam Topic 6)

What is the primary difference between regulations and standards?

- A. Standards will include regulations
- B. Standards that aren't followed are punishable by fines
- C. Regulations are made enforceable by the power provided by laws
- D. Regulations must be reviewed and approved by the business

**Answer:** C

#### NEW QUESTION 4

- (Exam Topic 6)

Devising controls for information security is a balance between?

- A. Governance and compliance
- B. Auditing and security
- C. Budget and risk tolerance
- D. Threats and vulnerabilities

**Answer:** C

#### **Explanation:**

Reference: [https://www.cybok.org/media/downloads/cybok\\_version\\_1.0.pdf](https://www.cybok.org/media/downloads/cybok_version_1.0.pdf)

#### NEW QUESTION 5

- (Exam Topic 6)

Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?

- A. Purge
- B. Clear
- C. Mangle
- D. Destroy

**Answer:** B

#### **Explanation:**

Reference:

<https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations>

#### NEW QUESTION 6

- (Exam Topic 6)

The primary responsibility for assigning entitlements to a network share lies with which role?

- A. CISO
- B. Data owner
- C. Chief Information Officer (CIO)

D. Security system administrator

**Answer:** B

**Explanation:**

Reference: <https://resources.infosecinstitute.com/certification/data-and-system-ownership/>

#### NEW QUESTION 7

- (Exam Topic 6)

A Security Operations Manager is finding it difficult to maintain adequate staff levels to monitor security operations during off-hours. To reduce the impact of staff shortages and increase coverage during off-hours, the SecOps manager is considering outsourcing off-hour coverage.

What Security Operations Center (SOC) model does this BEST describe?

- A. Virtual SOC
- B. In-house SOC
- C. Security Network Operations Center (SNOC)
- D. Hybrid SOC

**Answer:** A

**Explanation:**

Reference:

<https://www.techtarget.com/searchsecurity/tip/Benefits-of-virtual-SOCs-Enterprise-run-vs-fully-managed>

#### NEW QUESTION 8

- (Exam Topic 6)

A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

- A. Public cloud
- B. Private cloud
- C. Community cloud
- D. Hybrid cloud

**Answer:** D

**Explanation:**

Reference:

<https://www.datacenters.com/services/cloud-services#:~:text=Hybrid%20clouds%20combine%20public%20and>

#### NEW QUESTION 9

- (Exam Topic 6)

Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person's eye.

However, authorization failures can occur with individuals who have?

- A. Glaucoma or cataracts
- B. Two different colored eyes (heterochromia iridium)
- C. Contact lens
- D. Malaria

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 6)

A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP). In developing the business impact assessment (BIA), which of the following MOST closely relate to the data backup and restoral?

- A. Recovery Point Objective (RPO)
- B. Mean Time to Delivery (MTD)
- C. Recovery Time Objective (RTO)
- D. Maximum Tolerable Downtime (MTD)

**Answer:** C

**Explanation:**

Reference:

<https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#:~:text=The%2>

#### NEW QUESTION 10

- (Exam Topic 6)

The main purpose of the SOC is:

- A. An organization which provides Tier 1 support for technology issues and provides escalation when needed
- B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities
- C. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation
- D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware

**Answer:** C

**Explanation:**

Reference: <https://www.eccouncil.org/what-is-soc/>

**NEW QUESTION 13**

- (Exam Topic 6)

What key technology can mitigate ransomware threats?

- A. Use immutable data storage
- B. Phishing exercises
- C. Application of multiple end point anti-malware solutions
- D. Blocking use of wireless networks

**Answer:** A

**Explanation:**

Reference:

<https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks>

**NEW QUESTION 15**

- (Exam Topic 6)

The Board of Directors of a publicly-traded company is concerned about the security implications of a strategic project that will migrate 50% of the organization's information technology assets to the cloud. They have requested a briefing on the project plan and a progress report of the security stream of the project. As the CISO, you have been tasked with preparing the report for the Chief Executive Officer to present.

Using the Earned Value Management (EVM), what does a Cost Variance (CV) of -1,200 mean?

- A. The project is over budget
- B. The project budget has reserves
- C. The project cost is in alignment with the budget
- D. The project is under budget

**Answer:** A

**Explanation:**

Reference:

<https://www.pmi.org/learning/library/earned-value-management-systems-analysis-8026#:~:text=The%20cost%2>

**NEW QUESTION 19**

- (Exam Topic 6)

What does RACI stand for?

- A. Reasonable, Actionable, Controlled, and Implemented
- B. Responsible, Actors, Consult, and Instigate
- C. Responsible, Accountable, Consulted, and Informed
- D. Review, Act, Communicate, and Inform

**Answer:** C

**Explanation:**

Reference: <https://www.google.com/search?q=What+does+RACI+stand+for&oq=What+does+RACI+stand+for&aqs=edge>

**NEW QUESTION 22**

- (Exam Topic 6)

Which of the following are the triple constraints of project management?

- A. Time, quality, and scope
- B. Cost, quality, and time
- C. Scope, time, and cost
- D. Quality, scope, and cost

**Answer:** C

**Explanation:**

Reference:

<https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%>

**NEW QUESTION 24**

- (Exam Topic 6)

An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.

What is the MOST likely reason why the sensitive data was posted?

- A. The DLP Solution was not integrated with mobile device anti-malware
- B. Data classification was not properly performed on the assets
- C. The sensitive data was not encrypted while at rest
- D. A risk assessment was not performed after purchasing the DLP solution

**Answer:** D

**NEW QUESTION 27**

- (Exam Topic 6)

What is a Statement of Objectives (SOA)?

- A. A section of a contract that defines tasks to be performed under said contract
- B. An outline of what the military will do during war
- C. A document that outlines specific desired outcomes as part of a request for proposal
- D. Business guidance provided by the CEO

**Answer:** A

**NEW QUESTION 28**

- (Exam Topic 6)

When performing a forensic investigation, what are the two MOST common data sources for obtaining evidence from a computer and mobile devices?

- A. RAM and unallocated space
- B. Unallocated space and RAM
- C. Slack space and browser cache
- D. Persistent and volatile data

**Answer:** D

**Explanation:**

Reference: <https://study.com/academy/lesson/data-storage-formats-digital-forensics-devices-types.html>

**NEW QUESTION 32**

- (Exam Topic 6)

A bastion host should be placed:

- A. Inside the DMZ
- B. In-line with the data center firewall
- C. Beyond the outer perimeter firewall
- D. As the gatekeeper to the organization's honeynet

**Answer:** C

**Explanation:**

Reference: <https://www.skillset.com/questions/a-bastion-host-is-which-of-the-following>

**NEW QUESTION 34**

- (Exam Topic 6)

When managing a project, the MOST important activity in managing the expectations of stakeholders is:

- A. To force stakeholders to commit ample resources to support the project
- B. To facilitate proper communication regarding outcomes
- C. To assure stakeholders commit to the project start and end dates in writing
- D. To finalize detailed scope of the project at project initiation

**Answer:** B

**Explanation:**

Reference:

<https://www.greycampus.com/blog/project-management/stakeholder-management-what-is-it-and-why-is-it-so-im>

**NEW QUESTION 38**

- (Exam Topic 6)

XYZ is a publicly-traded software development company.

Who is ultimately accountable to the shareholders in the event of a cybersecurity breach?

- A. Chief Financial Officer (CFO)
- B. Chief Software Architect (CIO)
- C. CISO
- D. Chief Executive Officer (CEO)

**Answer:** C

**Explanation:**

Reference: <https://www.eccouncil.org/information-security-management/>

**NEW QUESTION 40**

- (Exam Topic 6)

Which of the following is the MOST effective method to counter phishing attacks?

- A. User awareness and training

- B. Host based Intrusion Detection System (IPS)
- C. Acceptable use guide signed by all system users
- D. Antispam solution

**Answer:** A

**Explanation:**

Reference: <https://aware.eccouncil.org/4-best-ways-to-stop-phishing-with-security-awareness.html>

**NEW QUESTION 44**

- (Exam 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 45**

- (Exam 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 50**

- (Exam 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 51**

- (Exam 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 55**

- (Exam 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 56**

- (Exam 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 60**

- (Exam Topic 2)

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

- A. A substantive test of program library controls
- B. A compliance test of program library controls
- C. A compliance test of the program compiler controls
- D. A substantive test of the program compiler controls

**Answer: B**

**NEW QUESTION 64**

- (Exam Topic 2)

Control Objectives for Information and Related Technology (COBIT) is which of the following?

- A. An Information Security audit standard
- B. An audit guideline for certifying secure systems and controls
- C. A framework for Information Technology management and governance
- D. A set of international regulations for Information Technology governance

**Answer: C**

**NEW QUESTION 65**

- (Exam 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 69**

- (Exam 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 70**

- (Exam Topic 1)

An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

- A. Data breach disclosure
- B. Consumer right disclosure
- C. Security incident disclosure
- D. Special circumstance disclosure

**Answer: A**

**NEW QUESTION 75**

- (Exam 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 76**

- (Exam 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 77**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 79**

- (Exam 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 84**

- (Exam 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 88**

- (Exam Topic 1)

Which of the following is the MOST important benefit of an effective security governance process?

- A. Reduction of liability and overall risk to the organization
- B. Better vendor management
- C. Reduction of security breaches
- D. Senior management participation in the incident response process

**Answer:** A

**NEW QUESTION 90**

- (Exam 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 93**

- (Exam 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 96**

- (Exam 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 97**

- (Exam Topic 1)

What role should the CISO play in properly scoping a PCI environment?

- A. Validate the business units' suggestions as to what should be included in the scoping process
- B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment
- C. Ensure internal scope validation is completed and that an assessment has been done to discover all credit card data
- D. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope

**Answer:** C

**NEW QUESTION 100**

- (Exam 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 102**

- (Exam 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 106**

- (Exam 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 108**

- (Exam 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 112**

- (Exam 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 116**

- (Exam Topic 1)

What is the BEST way to achieve on-going compliance monitoring in an organization?

- A. Only check compliance right before the auditors are scheduled to arrive onsite.
- B. Outsource compliance to a 3rd party vendor and let them manage the program.
- C. Have Compliance and Information Security partner to correct issues as they arise.
- D. Have Compliance direct Information Security to fix issues after the auditors report.

**Answer: C**

#### **NEW QUESTION 117**

- (Exam Topic 1)

Who is responsible for securing networks during a security incident?

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

**Answer: D**

#### **NEW QUESTION 121**

- (Exam Topic 1)

Which of the following is MOST likely to be discretionary?

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

**Answer: C**

#### **NEW QUESTION 122**

- (Exam Topic 1)

An organization information security policy serves to

- A. establish budgetary input in order to meet compliance requirements
- B. establish acceptable systems and user behavior
- C. define security configurations for systems
- D. define relationships with external law enforcement agencies

**Answer: B**

#### **NEW QUESTION 125**

- (Exam 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 130**

- (Exam 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 131**

- (Exam 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 135

- (Exam 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 137

- (Exam 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 141

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 142

- (Exam 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 144

- (Exam Topic 1)

The exposure factor of a threat to your organization is defined by?

- A. Asset value times exposure factor
- B. Annual rate of occurrence
- C. Annual loss expectancy minus current cost of controls
- D. Percentage of loss experienced due to a realized threat event

**Answer: D**

#### NEW QUESTION 145

- (Exam 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 146

- (Exam Topic 1)

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

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

D. Communications Information

**Answer:** A

**NEW QUESTION 148**

- (Exam 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 152**

- (Exam 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 153**

- (Exam Topic 1)

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

- A. They are objective and can express risk / cost in real numbers
- B. They are subjective and can be completed more quickly
- C. They are objective and express risk / cost in approximates
- D. They are subjective and can express risk /cost in real numbers

**Answer:** A

**NEW QUESTION 157**

- (Exam 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 161**

- (Exam 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 163**

- (Exam 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 166**

- (Exam 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 171**

- (Exam Topic 1)

Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

- A. Risk management
- B. Security management
- C. Mitigation management
- D. Compliance management

**Answer:** D

**NEW QUESTION 173**

- (Exam Topic 1)

An organization's Information Security Policy is of MOST importance because

- A. it communicates management's commitment to protecting information resources
- B. it is formally acknowledged by all employees and vendors
- C. it defines a process to meet compliance requirements
- D. it establishes a framework to protect confidential information

**Answer:** A

**NEW QUESTION 174**

- (Exam 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 177**

- (Exam Topic 1)

Which of the following provides an audit framework?

- A. Control Objectives for IT (COBIT)
- B. Payment Card Industry-Data Security Standard (PCI-DSS)
- C. International Organization Standard (ISO) 27002
- D. National Institute of Standards and Technology (NIST) SP 800-30

**Answer:** A

**NEW QUESTION 180**

- (Exam 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 183**

- (Exam 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 186**

- (Exam 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 189

- (Exam Topic 6)

What are the common data hiding techniques used by criminals?

- A. Unallocated space and masking
- B. Website defacement and log manipulation
- C. Disabled Logging and admin elevation
- D. Encryption, Steganography, and Changing Metadata/Timestamps

**Answer:** D

#### Explanation:

Reference: <https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/>

#### NEW QUESTION 190

- (Exam Topic 6)

You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans. Which control is MOST important to protect AI products?

- A. Hash datasets
- B. Sanitize datasets
- C. Delete datasets
- D. Encrypt datasets

**Answer:** D

#### NEW QUESTION 195

- (Exam Topic 6)

What is an approach to estimating the strengths and weaknesses of alternatives used to determine options, which provide the BEST approach to achieving benefits while preserving savings called?

- A. Business Impact Analysis
- B. Economic Impact analysis
- C. Return on Investment
- D. Cost-benefit analysis

**Answer:** D

#### Explanation:

Reference: <https://artsandculture.google.com/entity/cost%E2%80%93benefit-analysis/m020w0x?hl=en>

#### NEW QUESTION 199

- (Exam Topic 6)

As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity. The performance quality audit activity is done in what project management process group?

- A. Executing
- B. Controlling
- C. Planning
- D. Closing

**Answer:** A

#### Explanation:

Reference:

<https://blog.masterofproject.com/executing-process-group-project-management/#:~:text=Executing%20Process>

#### NEW QUESTION 202

- (Exam Topic 6)

As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand. Which is the BEST type of risk that defines this event?

- A. Compliance Risk
- B. Reputation Risk
- C. Operational Risk
- D. Strategic Risk



**Answer:** B

**NEW QUESTION 203**

- (Exam 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 205**

- (Exam Topic 5)

Using the Transport Layer Security (TLS) protocol enables a client in a network to be:

- A. Provided with a digital signature
- B. Assured of the server's identity
- C. Identified by a network
- D. Registered by the server

**Answer:** B

**Explanation:**

Reference: <https://ukdiss.com/examples/tls.php>

**NEW QUESTION 208**

- (Exam 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 adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

- A. Annually
- B. Semi-annually
- C. Quarterly
- D. Never

**Answer:** D

**NEW QUESTION 210**

- (Exam Topic 5)

A digital signature addresses which of the following concerns?

- A. Message alteration
- B. Message copying
- C. Message theft
- D. Unauthorized reading

**Answer:** A

**Explanation:**

Reference: <https://www.entrust.com/resources/certificate-solutions/learn/digital-signatures>

**NEW QUESTION 214**

- (Exam Topic 5)

Which of the following information would MOST likely be reported at the board-level within an organization?

- A. System scanning trends and results as they pertain to insider and external threat sources
- B. The capabilities of a security program in terms of staffing support
- C. Significant risks and security incidents that have been discovered since the last assembly of the membership
- D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

**Answer:** C

**NEW QUESTION 218**

- (Exam Topic 5)

The rate of change in technology increases the importance of:

- A. Outsourcing the IT functions.



- B. Understanding user requirements.
- C. Hiring personnel with leading edge skills.
- D. Implementing and enforcing good processes.

**Answer:** D

#### NEW QUESTION 221

- (Exam Topic 5)

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years. Which of the following would be the FIRST step when addressing Information Security formally and consistently in this organization?

- A. Contract a third party to perform a security risk assessment
- B. Define formal roles and responsibilities for Internal audit functions
- C. Define formal roles and responsibilities for Information Security
- D. Create an executive security steering committee

**Answer:** C

#### NEW QUESTION 225

- (Exam Topic 5)

A CISO wants to change the defense strategy to ward off attackers. To accomplish this the CISO is looking to a strategy where attackers are lured into a zone of a safe network where attackers can be monitored, controlled, quarantined, or eradicated.

- A. Moderate investment
- B. Passive monitoring
- C. Integrated security controls
- D. Dynamic deception

**Answer:** D

#### NEW QUESTION 228

- (Exam Topic 5)

An organization has a number of Local Area Networks (LANs) linked to form a single Wide Area Network (WAN). Which of the following would BEST ensure network continuity?

- A. Third-party emergency repair contract
- B. Pre-built servers and routers
- C. Permanent alternative routing
- D. Full off-site backup of every server

**Answer:** C

#### NEW QUESTION 232

- (Exam 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 237

- (Exam Topic 5)

Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

- A. Segmentation controls.
- B. Shadow applications.
- C. Deception technology.
- D. Vulnerability management.

**Answer:** B

#### NEW QUESTION 238

- (Exam 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 241**

- (Exam 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 242**

- (Exam 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 243**

- (Exam 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 247**

- (Exam 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 248**

- (Exam Topic 5)

The primary purpose of a risk register is to:

- A. Maintain a log of discovered risks
- B. Track individual risk assessments
- C. Develop plans for mitigating identified risks
- D. Coordinate the timing of scheduled risk assessments

**Answer:** A

**Explanation:**

Reference: <https://sitemate.com/us/resources/articles/safety/purpose-of-a-risk-register/>

**NEW QUESTION 252**

- (Exam 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 254**

- (Exam Topic 5)

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

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

**Answer:** C

**NEW QUESTION 258**

- (Exam 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 261**

- (Exam Topic 5)

A newly-hired CISO needs to understand the organization's financial management standards for business units and operations. Which of the following would be the best source of this information?

- A. The internal accounting department
- B. The Chief Financial Officer (CFO)
- C. The external financial audit service
- D. The managers of the accounts payables and accounts receivables teams

**Answer:** D

**NEW QUESTION 262**

- (Exam 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 263**

- (Exam 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 268**

- (Exam 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 269**

- (Exam Topic 5)

As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

- A. Recovery Point Objective (RPO)
- B. Disaster Recovery Plan
- C. Recovery Time Objective (RTO)
- D. Business Continuity Plan

**Answer:** D

**Explanation:**

Reference: <https://www.resolver.com/resource/bcdr-metrics-that-matter/>

**NEW QUESTION 272**

- (Exam Topic 5)

At what level of governance are individual projects monitored and managed?

- A. Program
- B. Milestone
- C. Enterprise
- D. Portfolio

**Answer:** D

**NEW QUESTION 273**

- (Exam Topic 5)

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. Effective use of existing technologies
- B. Create a comprehensive security awareness program and provide success metrics to business units
- C. Proper budget management
- D. Leveraging existing implementations

**Answer:** B

**NEW QUESTION 276**

- (Exam Topic 5)

When project costs continually increase throughout implementation due to large or rapid changes in customer or user requirements, this is commonly known as:

- A. Cost/benefit adjustments
- B. Scope creep
- C. Prototype issues
- D. Expectations management

**Answer:** B

**Explanation:**

Reference:

[http://www.umsl.edu/~sauterv/analysis/6840\\_f03\\_papers/gurlen/](http://www.umsl.edu/~sauterv/analysis/6840_f03_papers/gurlen/)

**NEW QUESTION 281**

- (Exam 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 284**

- (Exam 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 285**

- (Exam 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 288**

- (Exam 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 293**

- (Exam Topic 5)

What is one key difference between Capital expenditures and Operating expenditures?

- A. Operating expense cannot be written off while Capital expense can
- B. Operating expenses can be depreciated over time and Capital expenses cannot
- C. Capital expenses cannot include salaries and Operating expenses can
- D. Capital expenditures allow for the cost to be depreciated over time and Operating does not

**Answer:** C

**NEW QUESTION 295**

- (Exam Topic 5)

Acceptable levels of information security risk tolerance in an organization should be determined by?

- A. Corporate legal counsel
- B. CISO with reference to the company goals
- C. CEO and board of director
- D. Corporate compliance committee

**Answer:** C

**NEW QUESTION 300**

- (Exam Topic 5)

Where does bottom-up financial planning primarily gain information for creating budgets?

- A. By adding all capital and operational costs from the prior budgetary cycle, and determining potential financial shortages
- B. By reviewing last year's program-level costs and adding a percentage of expected additional portfolio costs
- C. By adding the cost of all known individual tasks and projects that are planned for the next budgetary cycle
- D. By adding all planned operational expenses per quarter then summarizing them in a budget request

**Answer:** D

**NEW QUESTION 303**

- (Exam Topic 5)

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

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

**Answer:** B



#### NEW QUESTION 304

- (Exam Topic 5)

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

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

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

**Answer:** A

#### NEW QUESTION 309

- (Exam Topic 5)

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

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

**Answer:** B

#### NEW QUESTION 313

- (Exam Topic 5)

What is meant by password aging?

- A. An expiration date set for passwords
- B. A Single Sign-On requirement
- C. Time in seconds a user is allocated to change a password
- D. The amount of time it takes for a password to activate

**Answer:** C

#### Explanation:

Reference: <https://medical-dictionary.thefreedictionary.com/password+ageing>

#### NEW QUESTION 316

- (Exam Topic 5)

Which of the following best describes revenue?

- A. Non-operating financial liabilities minus expenses
- B. The true profit-making potential of an organization
- C. The sum value of all assets and cash flow into the business
- D. The economic benefit derived by operating a business

**Answer:** D

#### Explanation:

Reference: <https://www.investopedia.com/terms/r/revenue.asp>

#### NEW QUESTION 317

- (Exam 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 320

- (Exam Topic 5)

If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the BEST control to safeguard data integrity?

- A. Backup to tape
- B. Maintain separate VM backups
- C. Backup to a remote location
- D. Increase VM replication frequency

**Answer:** B

#### Explanation:

Reference:

<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/is-audit-basics-backup-andrecovery>

#### NEW QUESTION 324

- (Exam Topic 5)

Which type of physical security control scan a person's external features through a digital video camera before granting access to a restricted area?

- A. Iris scan
- B. Retinal scan
- C. Facial recognition scan
- D. Signature kinetics scan

**Answer: C**

#### NEW QUESTION 326

- (Exam Topic 5)

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

You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?

- A. Get approval from the board of directors
- B. Screen potential vendor solutions
- C. Verify that the cost of mitigation is less than the risk
- D. Create a risk metrics for all unmitigated risks

**Answer: C**

#### NEW QUESTION 327

- (Exam 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 331

- (Exam 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 correct aligns with the company goals. What needs to be verified FIRST?

- A. Scope of the project
- B. Training of the personnel on the project
- C. Timeline of the project milestones
- D. Vendor for the project

**Answer: A**

#### NEW QUESTION 335

- (Exam Topic 5)

What is the difference between encryption and tokenization?

- A. Tokenization combined with hashing is always better than encryption
- B. Encryption can be mathematically reversed to provide the original information
- C. The token contains the all original information
- D. Tokenization can be mathematically reversed to provide the original information

**Answer: B**

#### Explanation:

Reference:

[http://library.ahima.org/doc?oid=104090#.X\\_dwWolR3eQ](http://library.ahima.org/doc?oid=104090#.X_dwWolR3eQ)

#### NEW QUESTION 340

- (Exam Topic 5)

A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website. This type of control is considered

- A. Zero-day attack mitigation
- B. Preventive detection control
- C. Corrective security control
- D. Dynamic blocking control

**Answer: C**



#### NEW QUESTION 341

- (Exam Topic 5)

Which of the following is the MOST logical method of deploying security controls within an organization?

- A. Obtain funding for all desired controls and then create project plans for implementation
- B. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult and costly controls
- C. Apply the least costly controls to demonstrate positive program activity
- D. Obtain business unit buy-in through close communication and coordination

**Answer:** B

#### NEW QUESTION 345

- (Exam Topic 5)

What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

- A. Internal Audit
- B. Corporate governance
- C. Risk Oversight
- D. Key Performance Indicators

**Answer:** B

#### Explanation:

Reference: <https://www.igi-global.com/dictionary/corporate-governance/5957>

#### NEW QUESTION 348

- (Exam Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. Once supervisors and data owners have approved requests, information system administrators will implement

- A. Technical control(s)
- B. Management control(s)
- C. Policy control(s)
- D. Operational control(s)

**Answer:** A

#### NEW QUESTION 349

- (Exam Topic 5)

Which type of scan is used on the eye to measure the layer of blood vessels?

- A. Facial recognition scan
- B. Iris scan
- C. Signature kinetics scan
- D. Retinal scan

**Answer:** D

#### NEW QUESTION 351

- (Exam Topic 5)

Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

- A. Reviewing system administrator logs
- B. Auditing configuration templates
- C. Checking vendor product releases
- D. Performing system scans

**Answer:** D

#### NEW QUESTION 356

- (Exam Topic 5)

Which technology can provide a computing environment without requiring a dedicated hardware backend?

- A. Mainframe server
- B. Virtual Desktop
- C. Thin client
- D. Virtual Local Area Network

**Answer:** B

#### NEW QUESTION 360

- (Exam Topic 5)

Which of the following would negatively impact a log analysis of a multinational organization?

- A. Centralized log management
- B. Encrypted log files in transit
- C. Each node set to local time
- D. Log aggregation agent each node

**Answer:** D

#### NEW QUESTION 363

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 367

- (Exam Topic 5)

Which of the following best describes an access control process that confirms the identity of the entity seeking access to a logical or physical area?

- A. Identification
- B. Authorization
- C. Authentication
- D. Accountability

**Answer:** B

#### NEW QUESTION 368

- (Exam Topic 5)

As the Chief Information Security Officer, you are performing an assessment of security posture to understand what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows to detect and actively stop vulnerability exploits and attacks?

- A. Gigamon
- B. Intrusion Prevention System
- C. Port Security
- D. Anti-virus

**Answer:** B

#### Explanation:

Reference: <https://searchsecurity.techtarget.com/definition/intrusion-prevention>

#### NEW QUESTION 371

- (Exam 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 372

- (Exam 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 374

- (Exam 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 377**

- (Exam Topic 4)

What type of attack requires the least amount of technical equipment and has the highest success rate?

- A. War driving
- B. Operating system attacks
- C. Social engineering
- D. Shrink wrap attack

**Answer:** C

**NEW QUESTION 380**

- (Exam 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 381**

- (Exam 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 385**

- (Exam 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 386**

- (Exam 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 387**

- (Exam 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 392**

- (Exam Topic 4)

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

- A. ' o 1=1 -
- B. ../../../../
- C. "DROPTABLE USERNAME"
- D. NOPS

**Answer:** A

#### NEW QUESTION 396

- (Exam Topic 4)

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

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

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

**Answer:** A

#### NEW QUESTION 401

- (Exam 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 403

- (Exam 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 406

- (Exam 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 sever 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 409

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 414

- (Exam 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 417**

- (Exam 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 419**

- (Exam 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 423**

- (Exam 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 425**

- (Exam Topic 3)

Which of the following best summarizes the primary goal of a security program?

- A. Provide security reporting to all levels of an organization
- B. Create effective security awareness to employees
- C. Manage risk within the organization
- D. Assure regulatory compliance

**Answer:** C

**NEW QUESTION 426**

- (Exam 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 427**

- (Exam 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 431**

- (Exam 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 434

- (Exam Topic 3)

Which of the following represents the best method of ensuring business unit alignment with security program requirements?

- A. Provide clear communication of security requirements throughout the organization
- B. Demonstrate executive support with written mandates for security policy adherence
- C. Create collaborative risk management approaches within the organization
- D. Perform increased audits of security processes and procedures

**Answer: C**

#### NEW QUESTION 439

- (Exam Topic 3)

In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

- A. Distance learning/Web seminars
- B. Formal Class
- C. One-One Training
- D. Self –Study (noncomputerized)

**Answer: D**

#### NEW QUESTION 444

- (Exam 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 449

- (Exam Topic 3)

Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

- A. Risk Management
- B. Risk Assessment
- C. System Testing
- D. Vulnerability Assessment

**Answer: B**

#### NEW QUESTION 454

- (Exam 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 455

- (Exam Topic 3)

Which of the following is considered one of the most frequent failures in project management?

- A. Overly restrictive management
- B. Excessive personnel on project
- C. Failure to meet project deadlines
- D. Insufficient resources

**Answer: C**



**NEW QUESTION 459**

- (Exam Topic 3)

Which of the following is the MOST important component of any change management process?

- A. Scheduling
- B. Back-out procedures
- C. Outage planning
- D. Management approval

**Answer: D**

**NEW QUESTION 460**

- (Exam 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 465**

- (Exam 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 466**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 467**

- (Exam Topic 3)

Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement. What type of risk tolerance is Acme exhibiting? (choose the BEST answer):

- A. low risk-tolerance
- B. high risk-tolerance
- C. moderate risk-tolerance
- D. medium-high risk-tolerance

**Answer: A**

**NEW QUESTION 469**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 474**

- (Exam 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 478**

- (Exam 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 479**

- (Exam 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 481**

- (Exam 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 482**

- (Exam 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 484**

- (Exam Topic 3)

Which of the following is the BEST indicator of a successful project?

- A. it is completed on time or early as compared to the baseline project plan
- B. it meets most of the specifications as outlined in the approved project definition
- C. it comes in at or below the expenditures planned for in the baseline budget
- D. the deliverables are accepted by the key stakeholders

**Answer:** D

**NEW QUESTION 485**

- (Exam 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 490**

- (Exam 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 494**

- (Exam Topic 3)

Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

- A. Terms and Conditions
- B. Service Level Agreements (SLA)
- C. Statement of Work
- D. Key Performance Indicators (KPI)

**Answer:** B

**NEW QUESTION 499**

- (Exam 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 502**

- (Exam 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 504**

- (Exam Topic 3)

You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

- A. Deploy a SEIM solution and have current staff review incidents first thing in the morning
- B. Contract with a managed security provider and have current staff on recall for incident response
- C. Configure your syslog to send SMS messages to current staff when target events are triggered
- D. Employ an assumption of breach protocol and defend only essential information resources

**Answer:** B

**NEW QUESTION 508**

- (Exam 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 509**

- (Exam 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 514

- (Exam Topic 3)

Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

- A. System testing
- B. Risk assessment
- C. Incident response
- D. Planning

**Answer:** A

#### NEW QUESTION 518

- (Exam 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 519

- (Exam 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 522

- (Exam 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 524

- (Exam 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 526

- (Exam 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 527

- (Exam Topic 2)

Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

- A. Single loss expectancy multiplied by the annual rate of occurrence
- B. Total loss expectancy multiplied by the total loss frequency
- C. Value of the asset multiplied by the loss expectancy

D. Replacement cost multiplied by the single loss expectancy

**Answer:** A

**NEW QUESTION 532**

- (Exam 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 535**

- (Exam 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 539**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 543**

- (Exam 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 548**

- (Exam 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 550**

- (Exam Topic 2)

Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

- A. Security Administrators
- B. Internal/External Audit
- C. Risk Management
- D. Security Operations

**Answer:** B

**NEW QUESTION 553**

- (Exam 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 556**

- (Exam 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 557**

- (Exam 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 559**

- (Exam Topic 2)

In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

- A. Internal Audit
- B. Database Administration
- C. Information Security
- D. Compliance

**Answer:** C

**NEW QUESTION 564**

- (Exam Topic 2)

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees. Which of the following can be used as a KPI?

- A. Number of callers who report security issues.
- B. Number of callers who report a lack of customer service from the call center
- C. Number of successful social engineering attempts on the call center
- D. Number of callers who abandon the call before speaking with a representative

**Answer:** C

**NEW QUESTION 565**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 567**

- (Exam Topic 2)

Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

- A. Control Objective for Information Technology (COBIT)
- B. Committee of Sponsoring Organizations (COSO)
- C. Payment Card Industry (PCI)
- D. Information Technology Infrastructure Library (ITIL)

**Answer:** A

**NEW QUESTION 571**

- (Exam 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 576**

- (Exam Topic 2)

The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is

- A. Penetration testers
- B. External Audit
- C. Internal Audit
- D. Forensic experts

**Answer:** B

**NEW QUESTION 577**

- (Exam 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 578**

- (Exam 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 583**

- (Exam 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 588**

- (Exam 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 589**

- (Exam Topic 2)

Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

- A. Meet regulatory compliance requirements
- B. Better understand the threats and vulnerabilities affecting the environment
- C. Better understand strengths and weaknesses of the program
- D. Meet legal requirements



**Answer:** C

**NEW QUESTION 592**

- (Exam Topic 2)

Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

- A. Perform a vulnerability scan of the network
- B. External penetration testing by a qualified third party
- C. Internal Firewall ruleset reviews
- D. Implement network intrusion prevention systems

**Answer:** B

**NEW QUESTION 596**

- (Exam 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 599**

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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 First Try
- \* 712-50 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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