

# 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)

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 3

- (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 4

- (Exam Topic 6)

From the CISO's perspective in looking at financial statements, the statement of retained earnings of an organization:

- A. Has a direct correlation with the CISO's budget
- B. Represents, in part, the savings generated by the proper acquisition and implementation of security controls
- C. Represents the sum of all capital expenditures
- D. Represents the percentage of earnings that could in part be used to finance future security controls

**Answer: D**

#### Explanation:

Reference: <https://www.investopedia.com/terms/s/statement-of-retained-earnings.asp>

#### NEW QUESTION 5

- (Exam Topic 6)

When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

- A. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
- B. Contracting rules typically require you to have conversations with two or more groups
- C. Discussing decisions with a very large group of people always provides a better outcome
- D. It helps to avoid regulatory or internal compliance issues

**Answer: D**

#### Explanation:

Reference:

<https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf>

#### NEW QUESTION 6

- (Exam Topic 6)

Which of the following strategies provides the BEST response to a ransomware attack?

- A. Real-time off-site replication
- B. Daily incremental backup
- C. Daily full backup
- D. Daily differential backup

**Answer:** B

#### NEW QUESTION 7

- (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 restore?

- 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 8

- (Exam Topic 6)

Of the following types of SOCs (Security Operations Centers), which one would be MOST likely used if the CISO has decided to outsource the infrastructure and administration of it?

- A. Virtual
- B. Dedicated
- C. Fusion
- D. Command

**Answer:** A

#### Explanation:

Reference: <https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC>

#### NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 6)

Who is responsible for verifying that audit directives are implemented?

- A. IT Management
- B. Internal Audit
- C. IT Security
- D. BOD Audit Committee

**Answer:** B

#### Explanation:

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

**NEW QUESTION 12**

- (Exam Topic 6)

In defining a strategic security plan for an organization, what should a CISO first analyze?

- A. Reach out to a business similar to yours and ask for their plan
- B. Set goals that are difficult to attain to drive more productivity
- C. Review business acquisitions for the past 3 years
- D. Analyze the broader organizational strategic plan

**Answer: D**

**Explanation:**

Reference: <https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/>

**NEW QUESTION 13**

- (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 15**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 16**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 17**

- (Exam Topic 2)

Which of the following activities is the MAIN purpose of the risk assessment process?

- A. Creating an inventory of information assets
- B. Classifying and organizing information assets into meaningful groups
- C. Assigning value to each information asset
- D. Calculating the risks to which assets are exposed in their current setting

**Answer: D**

**NEW QUESTION 21**

- (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 23**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 26**

- (Exam Topic 2)

The effectiveness of an audit is measured by?

- A. The number of actionable items in the recommendations
- B. How it exposes the risk tolerance of the company
- C. How the recommendations directly support the goals of the company
- D. The number of security controls the company has in use

**Answer:** C

**NEW QUESTION 27**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 30**

- (Exam Topic 2)

Which of the following is a fundamental component of an audit record?

- A. Date and time of the event
- B. Failure of the event
- C. Originating IP-Address
- D. Authentication type

**Answer:** A

**NEW QUESTION 32**

- (Exam Topic 2)

Which of the following are necessary to formulate responses to external audit findings?

- A. Internal Audit, Management, and Technical Staff
- B. Internal Audit, Budget Authority, Management
- C. Technical Staff, Budget Authority, Management
- D. Technical Staff, Internal Audit, Budget Authority

**Answer:** C

**NEW QUESTION 33**

- (Exam Topic 1)

What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

- A. Test every three years to ensure that things work as planned
- B. Conduct periodic tabletop exercises to refine the BC plan
- C. Outsource the creation and execution of the BC plan to a third party vendor
- D. Conduct a Disaster Recovery (DR) exercise every year to test the plan

**Answer:** B

**NEW QUESTION 35**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 37**

- (Exam Topic 1)

Developing effective security controls is a balance between:

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

**Answer: A**

**NEW QUESTION 40**

- (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 44**

- (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 49**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 54**

- (Exam Topic 1)

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

- A. Threat
- B. Vulnerability
- C. Attack vector
- D. Exploitation

**Answer: B**

**NEW QUESTION 57**

- (Exam Topic 1)

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

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

**Answer: A**

**NEW QUESTION 61**

- (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 63

- (Exam Topic 1)

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

- A. Multiple certifications, strong technical capabilities and lengthy resume
- B. Industry certifications, technical knowledge and program management skills
- C. College degree, audit capabilities and complex project management
- D. Multiple references, strong background check and industry certifications

**Answer: B**

### NEW QUESTION 64

- (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 68

- (Exam Topic 1)

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

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

**Answer: A**

### NEW QUESTION 71

- (Exam Topic 1)

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

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

**Answer: A**

### NEW QUESTION 72

- (Exam Topic 1)

You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

- A. Chief Information Security Officer
- B. Chief Executive Officer
- C. Chief Information Officer
- D. Chief Legal Counsel

**Answer: B**

### NEW QUESTION 75

- (Exam Topic 1)

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

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

**Answer: C**

### NEW QUESTION 79

- (Exam Topic 1)

Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

- A. Need to comply with breach disclosure laws
- B. Need to transfer the risk associated with hosting PII data
- C. Need to better understand the risk associated with using PII data
- D. Fiduciary responsibility to safeguard credit card information

**Answer: C**

**NEW QUESTION 80**

- (Exam Topic 1)

The PRIMARY objective of security awareness is to:

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

**Answer: B**

**NEW QUESTION 82**

- (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 84**

- (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 85**

- (Exam Topic 1)

Risk that remains after risk mitigation is known as

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

**Answer: B**

**NEW QUESTION 89**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 90**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 92**

- (Exam Topic 1)

When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

- A. The asset owner
- B. The asset manager
- C. The data custodian

D. The project manager

**Answer: A**

**NEW QUESTION 94**

- (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 95**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 99**

- (Exam Topic 1)

Information security policies should be reviewed:

- A. by stakeholders at least annually
- B. by the CISO when new systems are brought online
- C. by the Incident Response team after an audit
- D. by internal audit semiannually

**Answer: A**

**NEW QUESTION 101**

- (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 103**

- (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 104**

- (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 108**

- (Exam Topic 1)

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the

following standards and guidelines can BEST address this organization's need?

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

**Answer:** A

**NEW QUESTION 112**

- (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 114**

- (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 118**

- (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 121**

- (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 124**

- (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 127**

- (Exam Topic 1)

In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

- A. The organization uses exclusively a quantitative process to measure risk
- B. The organization uses exclusively a qualitative process to measure risk
- C. The organization's risk tolerance is high
- D. The organization's risk tolerance is lo

**Answer:** C

**NEW QUESTION 131**

- (Exam Topic 1)

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

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

**Answer: C**

**NEW QUESTION 134**

- (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 136**

- (Exam Topic 1)

A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

- A. Scan a representative sample of systems
- B. Perform the scans only during off-business hours
- C. Decrease the vulnerabilities within the scan tool settings
- D. Filter the scan output so only pertinent data is analyzed

**Answer: A**

**NEW QUESTION 141**

- (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 144**

- (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 148**

- (Exam Topic 1)

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

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

**Answer: A**

**NEW QUESTION 149**

- (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 150**

- (Exam Topic 1)

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

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

Answer: D

**NEW QUESTION 153**

- (Exam Topic 1)

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

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

Answer: A

**NEW QUESTION 155**

- (Exam Topic 1)

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

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

Answer: C

**NEW QUESTION 156**

- (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 161**

- (Exam Topic 6)

Many successful cyber-attacks currently include:

- A. Phishing Attacks
- B. Misconfigurations
- C. Social engineering
- D. All of these

Answer: C

**Explanation:**

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

**NEW QUESTION 166**

- (Exam Topic 6)

Which of the following statements below regarding Key Performance indicators (KPIs) are true?

- A. Development of KPI's are most useful when done independently
- B. They are a strictly quantitative measure of success
- C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
- D. They are a strictly qualitative measure of success

Answer: A

**Explanation:**

Reference: <https://kpi.org/KPI-Basics/KPI-Development>

**NEW QUESTION 171**

- (Exam Topic 6)

With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

- A. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
- B. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program
- C. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
- D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

**Answer: C**

**Explanation:**

Reference: [https://nanopdf.com/download/information-security-governance-guidance-for-boards-of\\_pdf](https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf) (9)

**NEW QUESTION 175**

- (Exam Topic 6)

To make sure that the actions of all employees, applications, and systems follow the organization's rules and regulations can BEST be described as which of the following?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 176**

- (Exam Topic 6)

Who should be involved in the development of an internal campaign to address email phishing?

- A. Business unit leaders, CIO, CEO
- B. Business Unit Leaders, CISO, CIO and CEO
- C. All employees
- D. CFO, CEO, CIO

**Answer: B**

**NEW QUESTION 177**

- (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 179**

- (Exam Topic 6)

What is a key policy that should be part of the information security plan?

- A. Account management policy
- B. Training policy
- C. Acceptable Use policy
- D. Remote Access policy

**Answer: C**

**Explanation:**

Reference: <https://www.exabeam.com/information-security/information-security-policy/>

#### NEW QUESTION 182

- (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.”

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

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

**Answer: B**

#### NEW QUESTION 183

- (Exam Topic 5)

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

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

**Answer: B**

#### NEW QUESTION 184

- (Exam Topic 5)

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

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

**Answer: C**

#### NEW QUESTION 186

- (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 188

- (Exam Topic 5)

A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company's building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

- A. Shoulder surfing
- B. Tailgating
- C. Social engineering
- D. Mantrap

**Answer: B**

#### NEW QUESTION 190

- (Exam Topic 5)

What are the three hierarchically related aspects of strategic planning and in which order should they be done?

- A. 1) Information technology strategic planning, 2) Enterprise strategic planning, 3) Cybersecurity or information security strategic planning
- B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3) Information technology strategic planning
- C. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning
- D. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3) Information technology strategic planning

**Answer: D**

#### NEW QUESTION 195

- (Exam Topic 5)

The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

- A. Video surveillance

- B. Mantrap
- C. Bollards
- D. Fence

**Answer:** D

**NEW QUESTION 196**

- (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.

In what phase of the response will the team extract information from the affected systems without altering original data?

- A. Response
- B. Investigation
- C. Recovery
- D. Follow-up

**Answer:** B

**NEW QUESTION 197**

- (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 202**

- (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 205**

- (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 frameworks and standards will BEST fit the organization as a baseline for their security program?

- A. NIST and Privacy Regulations
- B. ISO 27000 and Payment Card Industry Data Security Standards
- C. NIST and data breach notification laws
- D. ISO 27000 and Human resources best practices

**Answer:** B

**NEW QUESTION 206**

- (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. This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?

- A. International encryption restrictions
- B. Compliance to Payment Card Industry (PCI) data security standards
- C. Compliance with local government privacy laws
- D. Adherence to local data breach notification laws

**Answer:** B

**NEW QUESTION 209**

- (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 212**

- (Exam Topic 5)

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

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

**Answer: A**

**NEW QUESTION 213**

- (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 215**

- (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 216**

- (Exam Topic 5)

During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

- A. The budget is in a temporary state of imbalance
- B. The budget is operating at a deficit
- C. She can realign the budget through moderate capital expense (CAPEX) allocation
- D. She has a surplus of operational expenses (OPEX)

**Answer: A**

**NEW QUESTION 219**

- (Exam Topic 5)

Which of the following best describes a portfolio?

- A. The portfolio is used to manage and track individual projects
- B. The portfolio is used to manage incidents and events
- C. A portfolio typically consists of several programs
- D. A portfolio delivers one specific service or program to the business

**Answer: C**

**NEW QUESTION 220**

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

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

**Answer: B**

**NEW QUESTION 223**

- (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.

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

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

**Answer: B**

**NEW QUESTION 227**

- (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 231**

- (Exam Topic 5)

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

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

**Answer: B**

**NEW QUESTION 235**

- (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 237**

- (Exam Topic 5)

What is the primary reason for performing vendor management?

- A. To understand the risk coverage that are being mitigated by the vendor
- B. To establish a vendor selection process
- C. To document the relationship between the company and the vendor
- D. To define the partnership for long-term success

**Answer: A**

**NEW QUESTION 239**

- (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 241**

- (Exam Topic 5)

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door

open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

- A. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door
- B. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
- C. Educate and enforce physical security policies of the company to all the employees on a regular basis
- D. Setup a mock video camera next to the special card reader adjacent to the secure door

**Answer: C**

#### **NEW QUESTION 246**

- (Exam Topic 5)

Which of the following terms is used to describe countermeasures implemented to minimize risks to physical property, information, and computing systems?

- A. Security frameworks
- B. Security policies
- C. Security awareness
- D. Security controls

**Answer: D**

#### **Explanation:**

Reference: <https://www.ibm.com/cloud/learn/security-controls>

#### **NEW QUESTION 247**

- (Exam Topic 5)

Which of the following is the MOST important reason for performing assessments of the security portfolio?

- A. To assure that the portfolio is aligned to the needs of the broader organization
- B. To create executive support of the portfolio
- C. To discover new technologies and processes for implementation within the portfolio
- D. To provide independent 3rd party reviews of security effectiveness

**Answer: A**

#### **NEW QUESTION 251**

- (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 256**

- (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 correctly aligns with the company goals and the scope of the project is correct. What is the NEXT step?

- A. Review time schedules
- B. Verify budget
- C. Verify resources
- D. Verify constraints

**Answer: C**

#### **NEW QUESTION 261**

- (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 264**

- (Exam Topic 5)

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

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

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

**Answer:** A

**NEW QUESTION 266**

- (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 268**

- (Exam Topic 5)

Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

- A. Rights collision
- B. Excessive privileges
- C. Privilege creep
- D. Least privileges

**Answer:** B

**NEW QUESTION 270**

- (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 275**

- (Exam Topic 5)

A CISO has implemented a risk management capability within the security portfolio. Which of the following terms best describes this functionality?

- A. Service
- B. Program
- C. Portfolio
- D. Cost center

**Answer:** B

**NEW QUESTION 276**

- (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.

What phase of the response provides measures to reduce the likelihood of an incident from recurring?

- A. Response
- B. Investigation
- C. Recovery
- D. Follow-up

**Answer:** D

**NEW QUESTION 280**

- (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 281**

- (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. The organization wants a more permanent solution to the threat to user credential compromise through phishing. What technical solution would BEST address this issue?

- A. Professional user education on phishing conducted by a reputable vendor
- B. Multi-factor authentication employing hard tokens
- C. Forcing password changes every 90 days
- D. Decreasing the number of employees with administrator privileges

**Answer: B**

**NEW QUESTION 284**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 289**

- (Exam Topic 4)

The process of creating a system which divides documents based on their security level to manage access to private data is known as

- A. security coding
- B. data security system
- C. data classification
- D. privacy protection

**Answer: C**

**NEW QUESTION 293**

- (Exam Topic 4)

Physical security measures typically include which of the following components?

- A. Physical, Technical, Operational
- B. Technical, Strong Password, Operational
- C. Operational, Biometric, Physical
- D. Strong password, Biometric, Common Access Card

**Answer: A**

**NEW QUESTION 296**

- (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 301**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 303**

- (Exam Topic 4)

An anonymity network is a series of?

- A. Covert government networks
- B. War driving maps
- C. Government networks in Tora
- D. Virtual network tunnels

**Answer: D**

**NEW QUESTION 307**

- (Exam Topic 4)

While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

- A. Enterprise Risk Assessment
- B. Disaster recovery strategic plan
- C. Business continuity plan
- D. Application mapping document

**Answer: B**

**NEW QUESTION 310**

- (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 312**

- (Exam Topic 4)

Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?

- A. Comprehensive Log-Files from all servers and network devices affected during the attack
- B. Fully trained network forensic experts to analyze all data right after the attack
- C. Uninterrupted Chain of Custody
- D. Expert forensics witness

**Answer: C**

**NEW QUESTION 317**

- (Exam Topic 4)

Which of the following backup sites takes the longest recovery time?

- A. Cold site
- B. Hot site
- C. Warm site
- D. Mobile backup site

**Answer: A**

**NEW QUESTION 322**

- (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 324**

- (Exam Topic 4)

Which of the following statements about Encapsulating Security Payload (ESP) is true?

- A. It is an IPSec protocol.
- B. It is a text-based communication protocol.
- C. It uses TCP port 22 as the default port and operates at the application layer.
- D. It uses UDP port 22

**Answer:** A

**NEW QUESTION 329**

- (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 333**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 336**

- (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 341**

- (Exam Topic 3)

The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

- A. Work with the IT group and tell them to put IPS in-line and say it won't cause any network impact
- B. Explain to the IT group that the IPS won't cause any network impact because it will fail open
- C. Explain to the IT group that this is a business need and the IPS will fail open however, if there is a network failure the CISO will accept responsibility
- D. Explain to the IT group that the IPS will fail open once in-line however it will be deployed in monitor mode for a set period of time to ensure that it doesn't block any legitimate traffic

**Answer:** D

**NEW QUESTION 343**

- (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 347**

- (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 352**

- (Exam Topic 3)

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

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

**Answer: A**

#### **NEW QUESTION 355**

- (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 360**

- (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 361**

- (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 364**

- (Exam Topic 3)

An example of professional unethical behavior is:

- A. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation
- B. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
- C. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
- D. Storing client lists and other sensitive corporate internal documents on a removable thumb drive

**Answer: C**

#### **NEW QUESTION 368**

- (Exam Topic 3)

Risk appetite is typically determined by which of the following organizational functions?

- A. Security
- B. Business units
- C. Board of Directors
- D. Audit and compliance

**Answer: C**

**NEW QUESTION 373**

- (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 378**

- (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 380**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 385**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 389**

- (Exam Topic 3)

Which of the following is critical in creating a security program aligned with an organization's goals?

- A. Ensure security budgets enable technical acquisition and resource allocation based on internal compliance requirements
- B. Develop a culture in which users, managers and IT professionals all make good decisions about information risk
- C. Provide clear communication of security program support requirements and audit schedules
- D. Create security awareness programs that include clear definition of security program goals and charters

**Answer: B**

**NEW QUESTION 390**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 392**

- (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 397**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 398**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 402**

- (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 404**

- (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 407**

- (Exam Topic 2)

The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

- A. assign the responsibility to the information security team.
- B. assign the responsibility to the team responsible for the management of the controls.
- C. create operational reports on the effectiveness of the controls.
- D. perform an independent audit of the security controls.

**Answer:** D

**NEW QUESTION 408**

- (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 411**

- (Exam Topic 2)

Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

- A. Detective Controls
- B. Proactive Controls
- C. Preemptive Controls
- D. Organizational Controls

**Answer: D**

#### NEW QUESTION 413

- (Exam Topic 2)

Which of the following are primary concerns for management with regard to assessing internal control objectives?

- A. Confidentiality, Availability, Integrity
- B. Compliance, Effectiveness, Efficiency
- C. Communication, Reliability, Cost
- D. Confidentiality, Compliance, Cost

**Answer: B**

#### NEW QUESTION 414

- (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 415

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 418

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 419

- (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 423

- (Exam Topic 2)

As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?

- A. Nothing, this falls outside your area of influence.
- B. Close and chain the door shut and send a company-wide memo banning the practice.
- C. Have a risk assessment performed.
- D. Post a guard at the door to maintain physical security

**Answer: C**

**NEW QUESTION 426**

- (Exam Topic 2)

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

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

**Answer: B**

**NEW QUESTION 429**

- (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 430**

- (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 434**

- (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 437**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 441**

- (Exam Topic 2)

You have implemented the new controls. What is the next step?

- A. Document the process for the stakeholders
- B. Monitor the effectiveness of the controls
- C. Update the audit findings report
- D. Perform a risk assessment

**Answer: B**

**NEW QUESTION 442**

- (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 445**

- (Exam Topic 2)

You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

- A. Validate that security awareness program content includes information about the potential vulnerability
- B. Conduct a thorough risk assessment against the current implementation to determine system functions
- C. Determine program ownership to implement compensating controls
- D. Send a report to executive peers and business unit owners detailing your suspicions

**Answer: B**

**NEW QUESTION 448**

- (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 450**

- (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 452**

- (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 454**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 459**

.....

## 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](#)