

## Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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



#### NEW QUESTION 1

- (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 2

- (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 3

- (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 4

- (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 5

- (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 6

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 7

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 8

- (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 9

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 10

- (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 10

- (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 11

- (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 13

- (Exam Topic 1)

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

- A. Strong authentication technologies
- B. Financial reporting regulations

- C. Credit card compliance and regulations
- D. Local privacy laws

**Answer:** D

#### NEW QUESTION 17

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 19

- (Exam Topic 1)

A method to transfer risk is to:

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

**Answer:** C

#### NEW QUESTION 24

- (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 26

- (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 27

- (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 28

- (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 32

- (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 33

- (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 34

- (Exam Topic 1)

Risk is defined as:

- A. Threat times vulnerability divided by control
- B. Advisory plus capability plus vulnerability
- C. Asset loss times likelihood of event
- D. Quantitative plus qualitative impact

**Answer:** A

### NEW QUESTION 39

- (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 42

- (Exam Topic 1)

What is the MAIN reason for conflicts between Information Technology and Information Security programs?

- A. Technology governance defines technology policies and standards while security governance does not.
- B. Security governance defines technology best practices and Information Technology governance does not.
- C. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
- D. The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.

**Answer:** D

### NEW QUESTION 47

- (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 52

- (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 57

- (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 59

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 61

- (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 64

- (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 65

- (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 68

- (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 72

- (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 76

- (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 78

- (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 83

- (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 87

- (Exam Topic 5)

Which of the following is a common technology for visual monitoring?

- A. Closed circuit television
- B. Open circuit television
- C. Blocked video
- D. Local video

**Answer:** A

**Explanation:**

Reference: <https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/>

#### NEW QUESTION 91

- (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 96**

- (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 99**

- (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 103**

- (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 105**

- (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 110**

- (Exam Topic 5)

Human resource planning for security professionals in your organization is a:

- A. Simple and easy task because the threats are getting easier to find and correct.
- B. Training requirement that is met through once every year user training.
- C. Training requirement that is on-going and always changing.
- D. Not needed because automation and anti-virus software has eliminated the threats.

**Answer: C**

**NEW QUESTION 113**

- (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 115

- (Exam Topic 5)

The newly appointed CISO of an organization is reviewing the IT security strategic plan. Which of the following is the MOST important component of the strategic plan?

- A. There is integration between IT security and business staffing.
- B. There is a clear definition of the IT security mission and vision.
- C. There is an auditing methodology in place.
- D. The plan requires return on investment for all security projects.

**Answer:** B

#### NEW QUESTION 120

- (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 121

- (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 125

- (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 127

- (Exam Topic 5)

A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

- A. Poorly configured firewalls
- B. Malware
- C. Advanced Persistent Threat (APT)
- D. An insider

**Answer:** D

#### NEW QUESTION 129

- (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 132

- (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 137

- (Exam Topic 5)

If the result of an NPV is positive, then the project should be selected. The net present value shows the present value of the project, based on the decisions taken for its selection. What is the net present value equal to?

- A. Net profit – per capita income
- B. Total investment – Discounted cash
- C. Average profit – Annual investment
- D. Initial investment – Future value

**Answer: C**

#### NEW QUESTION 138

- (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 141

- (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 142

- (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 145

- (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 148

- (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 152**

- (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 157**

- (Exam Topic 5)

As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

- A. File Transfer Protocol (FTP)
- B. Virtual Local Area Network (VLAN)
- C. Simple Mail Transfer Protocol
- D. Virtual Private Network (VPN)

**Answer:** D

**Explanation:**

Reference: <https://searchnetworking.techtarget.com/definition/virtual-private-network>

**NEW QUESTION 162**

- (Exam Topic 5)

Smith, the project manager for a larger multi-location firm, is leading a software project team that has 18 members, 5 of which are assigned to testing. Due to recent recommendations by an organizational quality audit team, the project manager is convinced to add a quality professional to lead to test team at additional cost to the project. The project manager is aware of the importance of communication for the success of the project and takes the step of introducing additional communication channels, making it more complex, in order to assure quality levels of the project. What will be the first project management document that Smith should change in order to accommodate additional communication channels?

- A. WBS document
- B. Scope statement
- C. Change control document
- D. Risk management plan

**Answer:** A

**NEW QUESTION 167**

- (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 172**

- (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 173**

- (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 175

- (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 177

- (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 181

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 183

- (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 186

- (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 188

- (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 190

- (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 195

- (Exam Topic 4)

Which wireless encryption technology makes use of temporal keys?

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

**Answer:** B

#### NEW QUESTION 198

- (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 203

- (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 207

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 208

- (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 212

- (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 217

- (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 220

- (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 221

- (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 223

- (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 228

- (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 229

- (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 232**

- (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 237**

- (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 242**

- (Exam Topic 3)

When managing the critical path of an IT security project, which of the following is MOST important?

- A. Knowing who all the stakeholders are.
- B. Knowing the people on the data center team.
- C. Knowing the threats to the organization.
- D. Knowing the milestones and timelines of deliverables.

**Answer:** D

**NEW QUESTION 245**

- (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 247**

- (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 250**

- (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 255**

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 258

- (Exam Topic 2)

Dataflow diagrams are used by IT auditors to:

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

**Answer:** C

#### NEW QUESTION 260

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 262

- (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 266

- (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 268

- (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 272

- (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 275**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 712-50 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 712-50 Product From:

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

## Money Back Guarantee

### 712-50 Practice Exam Features:

- \* 712-50 Questions and Answers Updated Frequently
- \* 712-50 Practice Questions Verified by Expert Senior Certified Staff
- \* 712-50 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 712-50 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year