

EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)



NEW QUESTION 1

- (Exam Topic 6)

What is the MOST critical output of the incident response process?

- A. A complete document of all involved team members and the support they provided
- B. Recovery of all data from affected systems
- C. Lessons learned from the incident, so they can be incorporated into the incident response processes
- D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: C

Explanation:

Reference: <https://www.eccouncil.org/incident-response-plan-phases/>

NEW QUESTION 2

- (Exam Topic 6)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 3

- (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 4

- (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 5

- (Exam Topic 6)

What does RACI stand for?

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

Answer: C

Explanation:

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

NEW QUESTION 6

- (Exam Topic 6)

Of the following types of SOC's (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 7

- (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 8

- (Exam Topic 6)

When reviewing a Solution as a Service (SaaS) provider's security health and posture, which key document should you review?

- A. SaaS provider's website certifications and representations (certs and reps)
- B. SOC-2 Report
- C. Metasploit Audit Report
- D. Statement from SaaS provider attesting their ability to secure your data

Answer: B

Explanation:

Reference: <https://www.threatstack.com/blog/how-saas-companies-can-build-a-compliance-roadmap>

NEW QUESTION 9

- (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 10

- (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 10

- (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 11

- (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 16

- (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 19

- (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 24

- (Exam Topic 1)

What two methods are used to assess risk impact?

- A. Cost and annual rate of expectance
- B. Subjective and Objective
- C. Qualitative and percent of loss realized
- D. Quantitative and qualitative

Answer: D

NEW QUESTION 25

- (Exam Topic 1)

One of the MAIN goals of a Business Continuity Plan is to

- A. Ensure all infrastructure and applications are available in the event of a disaster
- B. Allow all technical first-responders to understand their roles in the event of a disaster
- C. Provide step by step plans to recover business processes in the event of a disaster
- D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer: C

NEW QUESTION 30

- (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 31

- (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 32

- (Exam Topic 1)

What is the main purpose of the Incident Response Team?

- A. Ensure efficient recovery and reinstate repaired systems

- B. Create effective policies detailing program activities
- C. Communicate details of information security incidents
- D. Provide current employee awareness programs

Answer: A

NEW QUESTION 33

- (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 34

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 37

- (Exam Topic 1)

Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 41

- (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 43

- (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 45

- (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 50

- (Exam Topic 1)

The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

- A. Due Protection
- B. Due Care
- C. Due Compromise
- D. Due process

Answer: B

NEW QUESTION 53

- (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 57

- (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 58

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 60

- (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 62

- (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 67

- (Exam Topic 6)

When information security falls under the Chief Information Officer (CIO), what is their MOST essential role?

- A. Oversees the organization's day-to-day operations, creating the policies and strategies that govern operations
- B. Enlisting support from key executives the information security program budget and policies
- C. Charged with developing and implementing policies designed to protect employees and customers' data from unauthorized access
- D. Responsible for the success or failure of the IT organization and setting strategic direction

Answer: D

Explanation:

Reference: <https://www.investopedia.com/terms/c/cio.asp>

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 73

- (Exam Topic 6)

When evaluating a Managed Security Services Provider (MSSP), which service(s) is/are most important:

- A. Patch management
- B. Network monitoring
- C. Ability to provide security services tailored to the business' needs
- D. 24/7 tollfree number

Answer: C

Explanation:

Reference: <https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps>

NEW QUESTION 74

- (Exam Topic 6)

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

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

Answer: A

Explanation:

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

NEW QUESTION 79

- (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 82

- (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 86

- (Exam Topic 5)

A digital signature addresses which of the following concerns?

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

Answer: A

Explanation:

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

NEW QUESTION 90

- (Exam Topic 5)

What are the three stages of an identity and access management system?

- A. Authentication, Authorize, Validation
- B. Provision, Administration, Enforcement
- C. Administration, Validation, Protect
- D. Provision, Administration, Authentication

Answer: A

Explanation:

Reference: <https://digitalguardian.com/blog/what-identity-and-access-management-iam>

NEW QUESTION 92

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 94

- (Exam Topic 5)

The rate of change in technology increases the importance of:

- A. Outsourcing the IT functions.
- B. Understanding user requirements.
- C. Hiring personnel with leading edge skills.
- D. Implementing and enforcing good processes.

Answer: D

NEW QUESTION 95

- (Exam Topic 5)

When analyzing and forecasting a capital expense budget what are not included?

- A. Network connectivity costs
- B. New datacenter to operate from
- C. Upgrade of mainframe
- D. Purchase of new mobile devices to improve operations

Answer: A

NEW QUESTION 99

- (Exam Topic 5)

Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

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

Answer: A

NEW QUESTION 104

- (Exam Topic 5)

The ability to demand the implementation and management of security controls on third parties providing services to an organization is

- A. Security Governance
- B. Compliance management
- C. Vendor management
- D. Disaster recovery

Answer: C

NEW QUESTION 109

- (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 114

- (Exam Topic 5)

Which of the following defines the boundaries and scope of a risk assessment?

- A. The risk assessment schedule
- B. The risk assessment framework
- C. The risk assessment charter
- D. The assessment context

Answer: B

Explanation:

Reference: <https://cfocussoftware.com/risk-management-framework/know-your-boundary/>

NEW QUESTION 115

- (Exam Topic 5)

File Integrity Monitoring (FIM) is considered a

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

Answer: C

NEW QUESTION 117

- (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 121

- (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 124

- (Exam Topic 5)

When dealing with risk, the information security practitioner may choose to:

- A. assign
- B. transfer
- C. acknowledge
- D. defer

Answer: C

NEW QUESTION 127

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 132

- (Exam Topic 5)

Which of the following is an accurate description of a balance sheet?

- A. The percentage of earnings that are retained by the organization for reinvestment in the business
- B. The details of expenses and revenue over a long period of time
- C. A summarized statement of all assets and liabilities at a specific point in time
- D. A review of regulations and requirements impacting the business from a financial perspective

Answer: C

NEW QUESTION 135

- (Exam Topic 5)

Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

What action should you take FIRST?

- A. Destroy the repository of stolen data
- B. Contact your local law enforcement agency
- C. Consult with other C-Level executives to develop an action plan
- D. Contract with a credit reporting company for paid monitoring services for affected customers

Answer: C

NEW QUESTION 137

- (Exam Topic 5)

What is the difference between encryption and tokenization?

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

Answer: B

Explanation:

Reference:

http://library.ahima.org/doc?oid=104090#.X_dwWolR3eQ

NEW QUESTION 139

- (Exam Topic 5)

Annual Loss Expectancy is derived from the function of which two factors?

- A. Annual Rate of Occurrence and Asset Value
- B. Single Loss Expectancy and Exposure Factor
- C. Safeguard Value and Annual Rate of Occurrence
- D. Annual Rate of Occurrence and Single Loss Expectancy

Answer: D

NEW QUESTION 141

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 146

- (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 148

- (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 152

- (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 154

- (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 155

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 158

- (Exam Topic 5)

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

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

Answer: B

Explanation:

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

NEW QUESTION 163

- (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 168

- (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 173

- (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 175

- (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 178

- (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 183

- (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 186

- (Exam Topic 3)

An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in severe revenue disruptions. Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

- A. The CISO
- B. Audit and Compliance
- C. The CFO
- D. The business owner

Answer: D

NEW QUESTION 188

- (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 191

- (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 196

- (Exam Topic 3)

Which of the following is considered a project versus a managed process?

- A. monitoring external and internal environment during incident response
- B. ongoing risk assessments of routine operations
- C. continuous vulnerability assessment and vulnerability repair
- D. installation of a new firewall system

Answer: D

NEW QUESTION 197

- (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 201

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 203

- (Exam Topic 3)

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

- A. Alignment with the business
- B. Effective use of existing technologies
- C. Leveraging existing implementations
- D. Proper budget management

Answer: A

NEW QUESTION 204

- (Exam Topic 3)

An application vulnerability assessment has identified a security flaw in an application. This is a flaw that was previously identified and remediated on a prior release of the application. Which of the following is MOST likely the reason for this recurring issue?

- A. Ineffective configuration management controls
- B. Lack of change management controls
- C. Lack of version/source controls
- D. High turnover in the application development department

Answer: C

NEW QUESTION 205

- (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 210

- (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 213

- (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 214

- (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 215

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 216

- (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 218

- (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 219

- (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 220

- (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 222

- (Exam Topic 2)

The risk found after a control has been fully implemented is called:

- A. Residual Risk
- B. Total Risk
- C. Post implementation risk
- D. Transferred risk

Answer: A

NEW QUESTION 226

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 230

- (Exam Topic 2)

IT control objectives are useful to IT auditors as they provide the basis for understanding the:

- A. Desired results or purpose of implementing specific control procedures.
- B. The audit control checklist.
- C. Techniques for securing information.
- D. Security policy

Answer: A

NEW QUESTION 235

- (Exam Topic 2)

You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis. Which of the following activities will help you in this?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Risk mitigation
- D. Estimate activity duration

Answer: A

NEW QUESTION 240

- (Exam Topic 2)

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

- A. Have internal audit conduct another audit to see what has changed.
- B. Contract with an external audit company to conduct an unbiased audit

- C. Review the recommendations and follow up to see if audit implemented the changes
- D. Meet with audit team to determine a timeline for corrections

Answer: C

NEW QUESTION 242

- (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 246

- (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 250

.....

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](#)