

EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)



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

NEW QUESTION 3

- (Exam Topic 6)

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

- A. CISO
- B. Data owner
- C. Chief Information Officer (CIO)
- D. Security system administrator

Answer: B

Explanation:

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

NEW QUESTION 4

- (Exam Topic 6)

A Security Operations Manager is finding it difficult to maintain adequate staff levels to monitor security operations during off-hours. To reduce the impact of staff shortages and increase coverage during off-hours, the SecOps manager is considering outsourcing off-hour coverage. What Security Operations Center (SOC) model does this BEST describe?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 6)

A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

- A. Inability to export the private certificate/key
- B. It can double as physical identification at the DMV
- C. It has the user's photograph to help ID them
- D. It can be used as a secure flash drive

Answer: C

Explanation:

Reference: <https://www.securew2.com/blog/piv-personal-identity-verification>

NEW QUESTION 8

- (Exam Topic 6)

What organizational structure combines the functional and project structures to create a hybrid of the two?

- A. Traditional
- B. Composite
- C. Project
- D. Matrix

Answer: D

Explanation:

Reference: <https://www.knowledgehut.com/tutorials/project-management/organization-structures>

NEW QUESTION 9

- (Exam Topic 6)

The Board of Directors of a publicly-traded company is concerned about the security implications of a strategic project that will migrate 50% of the organization's information technology assets to the cloud. They have requested a briefing on the project plan and a progress report of the security stream of the project. As the CISO, you have been tasked with preparing the report for the Chief Executive Officer to present. Using the Earned Value Management (EVM), what does a Cost Variance (CV) of -1,200 mean?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 10

- (Exam Topic 6)

What does RACI stand for?

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

Answer: C

Explanation:

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

NEW QUESTION 10

- (Exam Topic 6)

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

- A. Time, quality, and scope
- B. Cost, quality, and time

- C. Scope, time, and cost
- D. Quality, scope, and cost

Answer: C

Explanation:

Reference:

[https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%](https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%20of%20view,which%20is%20the%20most%20important%20constraint%20to%20manage%20the%20project%20effectively.)

NEW QUESTION 12

- (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 13

- (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 18

- (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 23

- (Exam Topic 6)

ABC Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame. You would like to implement key performance indicators to mitigate the risk. Which metric would meet the requirement?

- A. Number of times third parties access critical information systems
- B. Number of systems with known vulnerabilities
- C. Number of users with elevated privileges
- D. Number of websites with weak or misconfigured certificates

Answer: C

NEW QUESTION 27

- (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 28

- (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 33

- (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 34

- (Exam Topic 2)

How often should an environment be monitored for cyber threats, risks, and exposures?

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

Answer: D

NEW QUESTION 38

- (Exam Topic 2)

Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

- A. Use within an organization to formulate security requirements and objectives
- B. Implementation of business-enabling information security
- C. Use within an organization to ensure compliance with laws and regulations
- D. To enable organizations that adopt it to obtain certifications

Answer: B

NEW QUESTION 39

- (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 44

- (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 47

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 48

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 53

- (Exam Topic 2)

To have accurate and effective information security policies how often should the CISO review the organization policies?

- A. Every 6 months
- B. Quarterly
- C. Before an audit
- D. At least once a year

Answer: D

NEW QUESTION 57

- (Exam Topic 2)

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

- A. An administrator with too much time on their hands.
- B. Putting undue time commitment on the system administrator.
- C. Supporting the concept of layered security
- D. Network segmentation.

Answer: C

NEW QUESTION 59

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 63

- (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 68

- (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 71

- (Exam Topic 1)

When choosing a risk mitigation method what is the MOST important factor?

- A. Approval from the board of directors
- B. Cost of the mitigation is less than the risk
- C. Metrics of mitigation method success
- D. Mitigation method complies with PCI regulations

Answer: B

NEW QUESTION 74

- (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 75

- (Exam Topic 1)

When managing the security architecture for your company you must consider:

- A. Security and IT Staff size
- B. Company Values
- C. Budget
- D. All of the above

Answer: D

NEW QUESTION 77

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 79

- (Exam Topic 1)

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 81

- (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 83

- (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 86

- (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 87

- (Exam Topic 1)

Which of the following is a benefit of information security governance?

- A. Questioning the trust in vendor relationships.
- B. Increasing the risk of decisions based on incomplete management information.
- C. Direct involvement of senior management in developing control processes
- D. Reduction of the potential for civil and legal liability

Answer: D

NEW QUESTION 88

- (Exam Topic 1)

A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

- A. Enforce the existing security standards and do not allow the deployment of the new technology.
- B. Amend the standard to permit the deployment.
- C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
- D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Answer: C

NEW QUESTION 90

- (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 93

- (Exam Topic 1)

After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

- A. Risk Tolerance
- B. Qualitative risk analysis
- C. Risk Appetite
- D. Quantitative risk analysis

Answer: D

NEW QUESTION 94

- (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 97

- (Exam Topic 1)

What is the definition of Risk in Information Security?

- A. Risk = Probability x Impact
- B. Risk = Threat x Probability
- C. Risk = Financial Impact x Probability
- D. Risk = Impact x Threat

Answer: A

NEW QUESTION 100

- (Exam Topic 1)

The PRIMARY objective for information security program development should be:

- A. Reducing the impact of the risk to the business.
- B. Establishing strategic alignment with business continuity requirements
- C. Establishing incident response programs.
- D. Identifying and implementing the best security solutions.

Answer: A

NEW QUESTION 102

- (Exam Topic 1)

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 105

- (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 106

- (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 107

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 108

- (Exam Topic 1)

An organization information security policy serves to

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

Answer: B

NEW QUESTION 110

- (Exam Topic 1)

You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

- A. Controlled mitigation effort
- B. Risk impact comparison
- C. Relative likelihood of event
- D. Comparative threat analysis

Answer: C

NEW QUESTION 112

- (Exam Topic 1)

An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

- A. A high threat environment
- B. A low risk tolerance environment
- C. A low vulnerability environment
- D. A high risk tolerance environment

Answer: D

NEW QUESTION 115

- (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 117

- (Exam Topic 1)

When dealing with a risk management process, asset classification is important because it will impact the overall:

- A. Threat identification
- B. Risk monitoring
- C. Risk treatment
- D. Risk tolerance

Answer: C

NEW QUESTION 121

- (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 122

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 124

- (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 127

- (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 129

- (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 132

- (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 137

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 139

- (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 142

- (Exam Topic 1)

Which of the following has the GREATEST impact on the implementation of an information security governance model?

- A. Organizational budget
- B. Distance between physical locations
- C. Number of employees
- D. Complexity of organizational structure

Answer: D

NEW QUESTION 146

- (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 150

- (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 152

- (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 156

- (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 160

- (Exam Topic 1)

Which of the following international standards can be BEST used to define a Risk Management process in an organization?

- A. National Institute for Standards and Technology 800-50 (NIST 800-50)
- B. International Organization for Standardizations – 27005 (ISO-27005)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations – 27004 (ISO-27004)

Answer: B

NEW QUESTION 162

- (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 165

- (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 167

- (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 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 (9)

NEW QUESTION 172

- (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 175

- (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 178

- (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 179

- (Exam Topic 6)

A CISO must conduct risk assessments using a method where the Chief Financial Officer (CFO) receives impact data in financial terms to use as input to select the proper level of coverage in a new cybersecurity insurance policy.

What is the MOST effective method of risk analysis to provide the CFO with the information required?

- A. Conduct a quantitative risk assessment
- B. Conduct a hybrid risk assessment
- C. Conduct a subjective risk assessment
- D. Conduct a qualitative risk assessment

Answer: D

NEW QUESTION 181

- (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 182

- (Exam Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. Recently, members of your organization have been targeted through a number of sophisticated phishing attempts and have compromised their system credentials. What action can you take to prevent the misuse of compromised credentials to change bank account information from outside your organization while still allowing employees to manage their bank information?

- A. Turn off VPN access for users originating from outside the country
- B. Enable monitoring on the VPN for suspicious activity
- C. Force a change of all passwords
- D. Block access to the Employee-Self Service application via VPN

Answer: D

NEW QUESTION 187

- (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 188

- (Exam Topic 5)

Which of the following is MOST useful when developing a business case for security initiatives?

- A. Budget forecasts
- B. Request for proposals
- C. Cost/benefit analysis
- D. Vendor management

Answer: C

NEW QUESTION 191

- (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 192

- (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: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs. The CISO discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-factor implementation project?

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

Answer: B

NEW QUESTION 201

- (Exam Topic 5)

As the CISO you need to write the IT security strategic plan. Which of the following is the MOST important to review before you start writing the plan?

- A. The existing IT environment.
- B. The company business plan.
- C. The present IT budget.
- D. Other corporate technology trends.

Answer: B

NEW QUESTION 203

- (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 208

- (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 209

- (Exam Topic 5)

As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

- A. Dual Control
- B. Separation of Duties
- C. Split Knowledge
- D. Least Privilege

Answer: A

Explanation:

Reference: <https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management>

NEW QUESTION 213

- (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 214

- (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.

From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?

- A. Lack of risk management process
- B. Lack of sponsorship from executive management
- C. IT security centric agenda
- D. Compliance centric agenda

Answer: C

NEW QUESTION 219

- (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 220

- (Exam Topic 5)

Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates. What is one proven method to account for common elements found within separate regulations and/or standards?

- A. Hire a GRC expert
- B. Use the Find function of your word processor
- C. Design your program to meet the strictest government standards
- D. Develop a crosswalk

Answer: D

NEW QUESTION 224

- (Exam Topic 5)

Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.

Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

- A. Scope
- B. Budget
- C. Resources
- D. Constraints

Answer: A

NEW QUESTION 225

- (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 228

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 232

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

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

Answer: A

NEW QUESTION 233

- (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 238

- (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 239

- (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 243

- (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 248

- (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 251

- (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 253

- (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 257

- (Exam Topic 5)

SCENARIO: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.

During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical aspect of the team's activities?

- A. Regular communication of incident status to executives
- B. Eradication of malware and system restoration
- C. Determination of the attack source
- D. Preservation of information

Answer: D

NEW QUESTION 258

- (Exam Topic 5)

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

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

Answer: D

Explanation:

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

NEW QUESTION 259

- (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 261

- (Exam Topic 5)

When updating the security strategic planning document what two items must be included?

- A. Alignment with the business goals and the vision of the CIO
- B. The risk tolerance of the company and the company mission statement
- C. The executive summary and vision of the board of directors
- D. The alignment with the business goals and the risk tolerance

Answer: D

NEW QUESTION 263

- (Exam Topic 5)

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

- A. Effective use of existing technologies

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

Answer: B

NEW QUESTION 264

- (Exam Topic 5)

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

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

- A. Lack of identification of technology stake holders
- B. Lack of business continuity process
- C. Lack of influence with leaders outside IT
- D. Lack of a security awareness program

Answer: C

NEW QUESTION 268

- (Exam Topic 5)

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

An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

- A. Controlled spear phishing campaigns
- B. Password changes
- C. Baselining of computer systems
- D. Scanning for viruses

Answer: A

NEW QUESTION 269

- (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 270

- (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 expense 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 273

- (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 278

- (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 283

- (Exam Topic 5)

Which of the following best describes revenue?

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

Answer: D

Explanation:

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

NEW QUESTION 284

- (Exam Topic 5)

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

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

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

Answer: B

NEW QUESTION 288

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 290

- (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 293

- (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 298

- (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 299

- (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 304

- (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 308

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 312

- (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 316

- (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 318

- (Exam Topic 5)

Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?

- A. Security regulations
- B. Asset classification
- C. Information security policy
- D. Data classification

Answer: C

NEW QUESTION 323

- (Exam Topic 5)

Which of the following is an accurate statement regarding capital expenses?

- A. They are easily reduced through the elimination of usage, such as reducing power for lighting of work areas during off-hours
- B. Capital expenses can never be replaced by operational expenses
- C. Capital expenses are typically long-term investments with value being realized through their use
- D. The organization is typically able to regain the initial cost by selling this type of asset

Answer: A

NEW QUESTION 326

- (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 330

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 332

- (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 337

- (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 339

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 340

- (Exam Topic 4)

A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?

- A. non-repudiation

- B. conflict resolution
- C. strong authentication
- D. digital rights management

Answer: A

NEW QUESTION 344

- (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 348

- (Exam Topic 4)

An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

- A. Shared key
- B. Asynchronous
- C. Open
- D. None

Answer: A

NEW QUESTION 349

- (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 350

- (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 354

- (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 358

- (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 363

- (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 366

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 367

- (Exam Topic 4)

You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

- A. Execute
- B. Read
- C. Administrator
- D. Public

Answer: D

NEW QUESTION 369

- (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 370

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 375

- (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 380

- (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 381

- (Exam Topic 3)

When is an application security development project complete?

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

Answer: A

NEW QUESTION 386

- (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 389

- (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 391

- (Exam Topic 3)

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

- A. Cost benefit
- B. Risk appetite
- C. Business continuity
- D. Likelihood of impact

Answer: B

NEW QUESTION 395

- (Exam Topic 3)

Your incident response plan should include which of the following?

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

Answer: C

NEW QUESTION 400

- (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 402

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 404

- (Exam Topic 3)

Your company has a “no right to privacy” notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee’s email account. What should you do? (choose the BEST answer):

- A. Grant her access, the employee has been adequately warned through the AUP.
- B. Assist her with the request, but only after her supervisor signs off on the action.
- C. Reset the employee’s password and give it to the supervisor.
- D. Deny the request citing national privacy laws.

Answer: B

NEW QUESTION 405

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 407

- (Exam Topic 3)

A stakeholder is a person or group:

- A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
- B. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
- C. That has budget authority.
- D. That will ultimately use the system.

Answer: A

NEW QUESTION 408

- (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 411

- (Exam Topic 3)

In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?

- A. Vmware, router, switch, firewall, syslog, vulnerability management system (VMS)
- B. Intrusion Detection System (IDS), firewall, switch, syslog
- C. Security Incident Event Management (SIEM), IDS, router, syslog
- D. SIEM, IDS, firewall, VMS

Answer: D

NEW QUESTION 415

- (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 420

- (Exam Topic 3)

When selecting a security solution with reoccurring maintenance costs after the first year, the CISO should: (choose the BEST answer)

- A. The CISO should cut other essential programs to ensure the new solution's continued use
- B. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
- C. Defer selection until the market improves and cash flow is positive
- D. Implement the solution and ask for the increased operating cost budget when it is time

Answer: B

NEW QUESTION 425

- (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 428

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 432

- (Exam Topic 3)

How often should the SSAE16 report of your vendors be reviewed?

- A. Quarterly
- B. Semi-annually
- C. Annually
- D. Bi-annually

Answer: C

NEW QUESTION 434

- (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 437

- (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 438

- (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 442

- (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 445

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 449

- (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 454

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 455

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 460

- (Exam Topic 2)

Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

- A. Servers, routers, switches, modem
- B. Firewall, exchange, web server, intrusion detection system (IDS)
- C. Firewall, anti-virus console, IDS, syslog
- D. IDS, syslog, router, switches

Answer: C

NEW QUESTION 461

- (Exam Topic 2)

The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

- A. The asset is more expensive than the remediation
- B. The audit finding is incorrect
- C. The asset being protected is less valuable than the remediation costs
- D. The remediation costs are irrelevant; it must be implemented regardless of cost.

Answer: C

NEW QUESTION 462

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 465

- (Exam Topic 2)

The regular review of a firewall ruleset is considered a

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

Answer: A

NEW QUESTION 469

- (Exam Topic 2)

Which of the following activities results in change requests?

- A. Preventive actions
- B. Inspection
- C. Defect repair
- D. Corrective actions

Answer: C

NEW QUESTION 473

- (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 476

- (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 480

- (Exam Topic 2)

Which of the following is the MOST important goal of risk management?

- A. Identifying the risk
- B. Finding economic balance between the impact of the risk and the cost of the control
- C. Identifying the victim of any potential exploits.
- D. Assessing the impact of potential threats

Answer: B

NEW QUESTION 481

- (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 484

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 485

- (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 487

- (Exam Topic 2)

Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

- A. Incident response plan
- B. Business Continuity plan
- C. Disaster recovery plan
- D. Damage control plan

Answer: C

NEW QUESTION 489

- (Exam Topic 2)

When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

- A. Threat Level, Risk of Compromise, and Consequences of Compromise
- B. Risk Avoidance, Threat Level, and Consequences of Compromise
- C. Risk Transfer, Reputational Impact, and Consequences of Compromise
- D. Reputational Impact, Financial Impact, and Risk of Compromise

Answer: A

NEW QUESTION 490

- (Exam Topic 2)

Which represents PROPER separation of duties in the corporate environment?

- A. Information Security and Identity Access Management teams perform two distinct functions
- B. Developers and Network teams both have admin rights on servers
- C. Finance has access to Human Resources data
- D. Information Security and Network teams perform two distinct functions

Answer: D

NEW QUESTION 491

- (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 493

- (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 498

- (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 501

- (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 503

.....

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](#)