712-50 Dumps

EC-Council Certified CISO (CCISO)

https://www.certleader.com/712-50-dumps.html
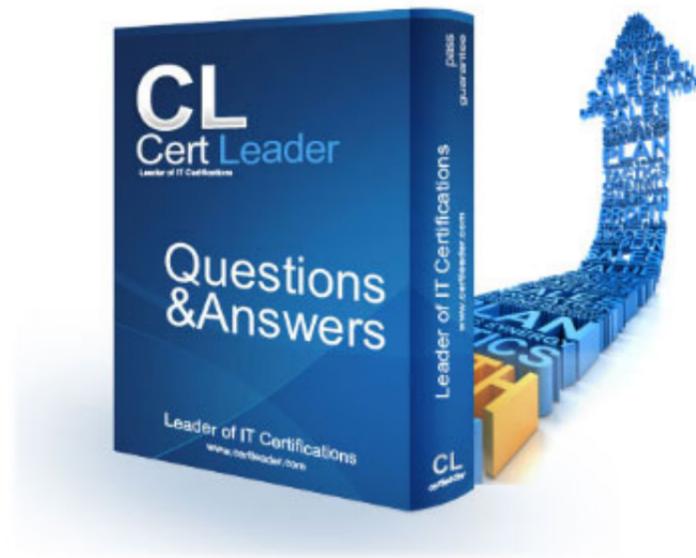
NEW QUESTION 1
- (Topic 1)
One of the MAIN goals of a Business Continuity Plan is to

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 2
- (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 3
- (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 4
- (Topic 1)
Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 5
- (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 6
- (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 7
- (Topic 1)
The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope
B. Getting authority to operate the system from executive management
C. Changing the default passwords
D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

NEW QUESTION 8
- (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 9
- (Topic 1)
What role should the CISO play in properly scoping a PCI environment?

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

Answer: :C

NEW QUESTION 10
- (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 10
- (Topic 1)
In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

A. High risk environments 6 months, low risk environments 12 months
B. Every 12 months
C. Every 18 months
D. Every six months

Answer: B

NEW QUESTION 12
- (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 13
- (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 18
- (Topic 1)
The Information Security Governance program MUST:

A. integrate with other organizational governance processes
B. support user choice for Bring Your Own Device (BYOD)
C. integrate with other organizational governance processes

D. show a return on investment for the organization

Answer: A

NEW QUESTION 23
- (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 26
- (Topic 1)
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer: A

NEW QUESTION 31
- (Topic 1)
The FIRST step in establishing a security governance program is to?

A. Conduct a risk assessment.
B. Obtain senior level sponsorship.
C. Conduct a workshop for all end users.
D. Prepare a security budget.

Answer: :B

NEW QUESTION 32
- (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 35
- (Topic 1)
Why is it vitally important that senior management endorse a security policy?

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.
D. So that they can be held legally accountable.

Answer: A

NEW QUESTION 37
- (Topic 1)
The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems
addressing low, moderate, and high levels of concern for

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

Answer: A

NEW QUESTION 40
- (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 42
- (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 44
- (Topic 1)
Which of the following should be determined while defining risk management strategies?

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

Answer: A

NEW QUESTION 48
- (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 51
- (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 55
- (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 56
- (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 57

- (Topic 1)
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

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

Answer: C

NEW QUESTION 61
- (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 62
- (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. I low vulnerability environment
D. A high risk tolerance environment

Answer: D

NEW QUESTION 64
- (Topic 1)
A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?

A. Audit validation
B. Physical control testing
C. Compliance management
D. Security awareness training

Answer: C

NEW QUESTION 65
- (Topic 1)
The single most important consideration to make when developing your security program, policies, and processes is:

A. Budgeting for unforeseen data compromises
B. Streamlining for efficiency
C. Alignment with the business
D. Establishing your authority as the Security Executive

Answer: C

NEW QUESTION 70
- (Topic 1)
The Information Security Management program MUST protect:

A. all organizational assets
B. critical business processes and /or revenue streams
C. intellectual property released into the public domain
D. against distributed denial of service attacks

Answer: B

NEW QUESTION 71
- (Topic 1)
Who is responsible for securing networks during a security incident?

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

Answer: D

NEW QUESTION 73
- (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 75
- (Topic 1)
Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

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

Answer: D

NEW QUESTION 78
- (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 80
- (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 81
- (Topic 1)
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

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

Answer: A

NEW QUESTION 86
- (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 88
- (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 89
- (Topic 2)
Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?

A. Systems logs
B. Hardware error reports
C. Utilization reports
D. Availability reports

Answer: D

NEW QUESTION 93
- (Topic 2)
You have implemented the new controls. What is the next step?

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

Answer: B

NEW QUESTION 96
- (Topic 2)
Which of the following are necessary to formulate responses to external audit findings?

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

Answer: C

NEW QUESTION 98
- (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 101
- (Topic 2)
Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

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

Answer: C

NEW QUESTION 103
- (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 104
- (Topic 2)
In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

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

Answer: C

NEW QUESTION 106
- (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 107
- (Topic 2)
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

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

Answer: B

NEW QUESTION 110
- (Topic 2)
Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

A. ISO 27001
B. ISO 27002
C. ISO 27004
D. ISO 27005

Answer: :D

NEW QUESTION 112
- (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 117
- (Topic 2)
Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

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

Answer: A

NEW QUESTION 119
- (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 122

- (Topic 2)
With respect to the audit management process, management response serves what function?

A. placing underperforming units on notice for failing to meet standards
B. determining whether or not resources will be allocated to remediate a finding
C. adding controls to ensure that proper oversight is achieved by management
D. revealing the "root cause" of the process failure and mitigating for all internal and external units

Answer: B

NEW QUESTION 124
- (Topic 2)
Which of the following activities must be completed BEFORE you can calculate risk?

A. Determining the likelihood that vulnerable systems will be attacked by specific threats
B. Calculating the risks to which assets are exposed in their current setting
C. Assigning a value to each information asset
D. Assessing the relative risk facing the organization's information assets

Answer: C

NEW QUESTION 128
- (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 130
- (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 132
- (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 133
- (Topic 2)
The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

A. Risk metrics
B. Management metrics
C. Operational metrics
D. Compliance metrics

Answer: C

NEW QUESTION 138
- (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 141
- (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 144
- (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 147
- (Topic 3)
When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

A. Type of data contained in the process/system
B. Type of connection/protocol used to transfer the data
C. Type of encryption required for the data once it is at rest
D. Type of computer the data is processed on

Answer: A

NEW QUESTION 148
- (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 149
- (Topic 3)
A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?

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

Answer: C

NEW QUESTION 150
- (Topic 3)
An organization has a stated requirement to block certain traffic on networks. The
implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in sever revenue disruptions. Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

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

Answer: D

NEW QUESTION 153

- (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 157
- (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 160
- (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 164
- (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 mangers
C. Security technicians
D. Security analysts

Answer: :B

NEW QUESTION 167
- (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 168
- (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 171
- (Topic 3)
You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

A. Deploy a SEIM solution and have current staff review incidents first thing in the morning
B. Contract with a managed security provider and have current staff on recall for incident response

C. Configure your syslog to send SMS messages to current staff when target events are triggered
D. Employ an assumption of breach protocol and defend only essential information resources

Answer: B

NEW QUESTION 175
- (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 179
- (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 184
- (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 189
- (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 193
- (Topic 3)
Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

A. Risk Assessment
B. Incident Response
C. Risk Management
D. Network Security administration

Answer: C

NEW QUESTION 198
- (Topic 3)
Which of the following represents the BEST method of ensuring security program alignment to business needs?

A. Create a comprehensive security awareness program and provide success metrics to business units
B. Create security consortiums, such as strategic security planning groups, that include business unit participation
C. Ensure security implementations include business unit testing and functional validation prior to production rollout
D. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role

Answer: B

NEW QUESTION 199

- (Topic 3)
What oversight should the information security team have in the change management process for application security?

A. Information security should be informed of changes to applications only
B. Development team should tell the information security team about any application security flaws
C. Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production
D. Information security should be aware of all application changes and work with developers before changes are deployed in production

Answer: C

NEW QUESTION 203
- (Topic 3)
When should IT security project management be outsourced?

A. When organizational resources are limited
B. When the benefits of outsourcing outweigh the inherent risks of outsourcing
C. On new, enterprise-wide security initiatives
D. On projects not forecasted in the yearly budget

Answer: B

NEW QUESTION 207
- (Topic 3)
Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

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

Answer: A

NEW QUESTION 212
- (Topic 3)
A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state. Which of the following security issues is the MOST likely reason leading to the audit findings?

A. Lack of asset management processes
B. Lack of change management processes
C. Lack of hardening standards
D. Lack of proper access controls

Answer: B

NEW QUESTION 213
- (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 217
- (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 218
- (Topic 3)
As the CISO for your company you are accountable for the protection of information resources commensurate with:

A. Customer demand
B. Cost and time to replace
C. Insurability tables
D. Risk of exposure

Answer: D

NEW QUESTION 223
- (Topic 3)
You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do. What is the BEST approach to handle this situation?

A. Tell the team to do their best and respond to each alert
B. Tune the sensors to help reduce false positives so the team can react better
C. Request additional resources to handle the workload
D. Tell the team to only respond to the critical and high alerts

Answer: B

NEW QUESTION 225
- (Topic 3)
To get an Information Security project back on schedule, which of the following will provide the MOST help?

A. Upper management support
B. More frequent project milestone meetings
C. Stakeholder support
D. Extend work hours

Answer: A

NEW QUESTION 226
- (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 227
- (Topic 4)
Which of the following is the MAIN security concern for public cloud computing?

A. Unable to control physical access to the servers
B. Unable to track log on activity
C. Unable to run anti-virus scans
D. Unable to patch systems as needed

Answer: A

NEW QUESTION 231
- (Topic 4)
The general ledger setup function in an enterprise resource package allows for setting accounting periods. Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

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

Answer: D

NEW QUESTION 235
- (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 239
- (Topic 4)
While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

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

Answer: B

NEW QUESTION 243
- (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 246
- (Topic 4)
SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 249
- (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 253
- (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 255
- (Topic 4)
Physical security measures typically include which of the following components?

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

Answer: A

NEW QUESTION 258
- (Topic 5)
Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
Symmetric encryption in general is preferable to asymmetric encryption when:

A. The number of unique communication links is large
B. The volume of data being transmitted is small
C. The speed of the encryption / deciphering process is essential
D. The distance to the end node is farthest away

Answer: C

NEW QUESTION 259

- (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. What type of control is being implemented by supervisors and data owners?

A. Management
B. Operational
C. Technical
D. Administrative

Answer: B

NEW QUESTION 260
- (Topic 5)
SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.
The CISO has implemented remediation activities. Which of the following is the MOST logical next step?

A. Validate the effectiveness of applied controls
B. Validate security program resource requirements
C. Report the audit findings and remediation status to business stake holders
D. Review security procedures to determine if they need modified according to findings

Answer: A

NEW QUESTION 264
- (Topic 5)
What is the primary reason for performing a return on investment analysis?

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

Answer: B

NEW QUESTION 267
- (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.
Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time. Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

A. Security Guards posted outside the Data Center
B. Data Loss Prevention (DLP)
C. Rigorous syslog reviews
D. Intrusion Detection Systems (IDS)

Answer: B

NEW QUESTION 269
- (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 273
- (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 276
- (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 278
- (Topic 5)
When creating contractual agreements and procurement processes why should security requirements be included?

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

Answer: B

NEW QUESTION 283
- (Topic 5)
SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.
The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning. Which of the following is the MOST logical next step?

A. Validate the effectiveness of current controls
B. Create detailed remediation funding and staffing plans
C. Report the audit findings and remediation status to business stake holders
D. Review security procedures to determine if they need modified according to findings

Answer: C

NEW QUESTION 287
- (Topic 5)
A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website. This type of control is considered

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

Answer: C

NEW QUESTION 290
- (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 292
- (Topic 5)
John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can John do in this instance?

A. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
B. Review the Request for Proposal (RFP) for guidance.
C. Withhold the vendor's payments until the issue is resolved.
D. Refer to the contract agreement for direction.

Answer: D

NEW QUESTION 297
- (Topic 5)
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers."
Which group of people should be consulted when developing your security program?

A. Peers
B. End Users
C. Executive Management
D. All of the above

Answer: :D

NEW QUESTION 299
- (Topic 5)
What is the primary reason for performing vendor management?

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

Answer: A

NEW QUESTION 300
- (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 302
- (Topic 5)
Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
How can you reduce the administrative burden of distributing symmetric keys for your employer?

A. Use asymmetric encryption for the automated distribution of the symmetric key
B. Use a self-generated key on both ends to eliminate the need for distribution
C. Use certificate authority to distribute private keys
D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

Answer: A

NEW QUESTION 307
- (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 309
- (Topic 5)
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.
Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

A. Upper management support
B. More frequent project milestone meetings
C. More training of staff members
D. Involve internal audit

Answer: A

NEW QUESTION 313
- (Topic 5)
Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:

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

Answer: B

NEW QUESTION 318
- (Topic 5)
Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

A. The Net Present Value (NPV) of the project is positive
B. The NPV of the project is negative
C. The Return on Investment (ROI) is larger than 10 months
D. The ROI is lower than 10 months

Answer: B

NEW QUESTION 322
- (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 324
- (Topic 5)
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.
Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

A. National Institute of Standards and Technology (NIST) Special Publication 800-53
B. Payment Card Industry Digital Security Standard (PCI DSS)
C. International Organization for Standardization – ISO 27001/2
D. British Standard 7799 (BS7799)

Answer: C

NEW QUESTION 328
- (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 330
- (Topic 5)
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers."
What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

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

Answer: B

NEW QUESTION 335
- (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 338
- (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-facto 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 341
- (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.
What is the MOST logical course of action the CISO should take?

A. Review the original solution set to determine if another system would fit the organization's risk appetite and budgetregulatory compliance requirements
B. Continue with the implementation and submit change requests to the vendor in order to ensure required functionality will be provided when needed
C. Continue with the project until the scalability issue is validated by others, such as an auditor or third party assessor
D. Cancel the project if the business need was based on internal requirements versus regulatory compliance requirements

Answer: A

NEW QUESTION 343
- (Topic 5)
The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

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

Answer: B

NEW QUESTION 348
- (Topic 5)
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.
When adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

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

Answer: D

NEW QUESTION 349
- (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 351
- (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 354
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 712-50 Exam with Our Prep Materials Via below:

https://www.certleader.com/712-50-dumps.html