

EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)



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)

Regulatory requirements typically force organizations to implement

- A. Mandatory controls
- B. Discretionary controls
- C. Optional controls
- D. Financial controls

Answer: A

NEW QUESTION 4

- (Topic 1)

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

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

Answer: C

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 9

- (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 10

- (Topic 1)

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

- A. When there is a need to develop a more unified incident response capability.
- B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
- C. When there is a variety of technologies deployed in the infrastructure.
- D. When it results in an overall lower cost of operating the security program.

Answer: B

NEW QUESTION 10

- (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 14

- (Topic 1)

Which of the following most commonly falls within the scope of an information security governance steering committee?

- A. Approving access to critical financial systems
- B. Developing content for security awareness programs
- C. Interviewing candidates for information security specialist positions
- D. Vetting information security policies

Answer: D

NEW QUESTION 15

- (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 19

- (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 21

- (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 25

- (Topic 1)

A method to transfer risk is to:

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

Answer: C

NEW QUESTION 26

- (Topic 1)

Risk appetite directly affects what part of a vulnerability management program?

- A. Staff
- B. Scope
- C. Schedule
- D. Scan tools

Answer: B

NEW QUESTION 27

- (Topic 1)

When briefing senior management on the creation of a governance process, the MOST important aspect should be:

- A. information security metrics.
- B. knowledge required to analyze each issue.
- C. baseline against which metrics are evaluated.
- D. linkage to business area objectives.

Answer: D

NEW QUESTION 30

- (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 35

- (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 39

- (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 42

- (Topic 1)

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

- A. Strong authentication technologies
- B. Financial reporting regulations
- C. Credit card compliance and regulations
- D. Local privacy laws

Answer: D

NEW QUESTION 46

- (Topic 1)

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

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

Answer: C

NEW QUESTION 48

- (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 52

- (Topic 1)

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

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

Answer: A

NEW QUESTION 53

- (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 57

- (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 61

- (Topic 1)

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

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

Answer: D

NEW QUESTION 66

- (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 69

- (Topic 1)

Risk that remains after risk mitigation is known as

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

Answer: B

NEW QUESTION 74

- (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 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 83

- (Topic 2)

An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

- A. Management Control
- B. Technical Control
- C. Training Control
- D. Operational Control

Answer: D

NEW QUESTION 85

- (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 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 90

- (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 95

- (Topic 2)

At which point should the identity access management team be notified of the termination of an employee?

- A. At the end of the day once the employee is off site
- B. During the monthly review cycle
- C. Immediately so the employee account(s) can be disabled
- D. Before an audit

Answer: C

NEW QUESTION 99

- (Topic 2)

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

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

Answer: D

NEW QUESTION 104

- (Topic 2)

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

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

Answer: C

NEW QUESTION 105

- (Topic 2)

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

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

Answer: A

NEW QUESTION 109

- (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 111

- (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 113

- (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 118

- (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 121

- (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 123

- (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 128

- (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 129

- (Topic 2)

Dataflow diagrams are used by IT auditors to:

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

Answer: C

NEW QUESTION 131

- (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 132

- (Topic 2)

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

- A. Senior Executives
- B. Office of the Auditor
- C. Office of the General Counsel
- D. All employees and users

Answer: A

NEW QUESTION 137

- (Topic 2)

An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application. What should be the NEXT step?

- A. Determine the annual loss expectancy (ALE)
- B. Create a crisis management plan
- C. Create technology recovery plans
- D. Build a secondary hot site

Answer: C

NEW QUESTION 140

- (Topic 2)

An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:

- A. Inform senior management of the risk involved.
- B. Agree to work with the security officer on these shifts as a form of preventative control.
- C. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
- D. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.

Answer: A

NEW QUESTION 142

- (Topic 2)

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

- A. Have internal audit conduct another audit to see what has changed.
- B. Contract with an external audit company to conduct an unbiased audit
- C. Review the recommendations and follow up to see if audit implemented the changes
- D. Meet with audit team to determine a timeline for corrections

Answer: C

NEW QUESTION 146

- (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 150

- (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 151

- (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 154

- (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 155

- (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 158

- (Topic 2)

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

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

Answer: D

NEW QUESTION 160

- (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 163

- (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 167

- (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 169

- (Topic 3)

Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

- A. Terms and Conditions
- B. Service Level Agreements (SLA)
- C. Statement of Work
- D. Key Performance Indicators (KPI)

Answer: B

NEW QUESTION 170

- (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 174

- (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 178

- (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 183

- (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 188

- (Topic 3)

A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability. What do you do?

- A. tell him to shut down the server
- B. tell him to call the police
- C. tell him to invoke the incident response process
- D. tell him to analyze the problem, preserve the evidence and provide a full analysis and report

Answer: C

NEW QUESTION 193

- (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 198

- (Topic 3)

Which of the following methodologies references the recommended industry standard that Information security project managers should follow?

- A. The Security Systems Development Life Cycle
- B. The Security Project And Management Methodology
- C. Project Management System Methodology
- D. Project Management Body of Knowledge

Answer: D

NEW QUESTION 202

- (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 204

- (Topic 3)

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

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

Answer: :D

NEW QUESTION 208

- (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 211

- (Topic 3)

Which of the following are not stakeholders of IT security projects?

- A. Board of directors
- B. Third party vendors
- C. CISO
- D. Help Desk

Answer: B

NEW QUESTION 215

- (Topic 3)

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

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

Answer: D

NEW QUESTION 216

- (Topic 3)

An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents. Which of the following would be considered a MAJOR constraint for the project?

- A. Time zone differences
- B. Compliance to local hiring laws
- C. Encryption import/export regulations
- D. Local customer privacy laws

Answer: C

NEW QUESTION 221

- (Topic 3)

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

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

Answer: C

NEW QUESTION 222

- (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 224

- (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 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 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 231

- (Topic 3)

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

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

Answer: B

NEW QUESTION 236

- (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 241

- (Topic 4)

In terms of supporting a forensic investigation, it is now imperative that managers, first- responders, etc., accomplish the following actions to the computer under investigation:

- A. Secure the area and shut-down the computer until investigators arrive
- B. Secure the area and attempt to maintain power until investigators arrive
- C. Immediately place hard drive and other components in an anti-static bag
- D. Secure the area.

Answer: B

NEW QUESTION 244

- (Topic 4)

One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys should be used to encrypt the message?

- A. Your public key
- B. The recipient's private key
- C. The recipient's public key
- D. Certificate authority key

Answer: C

NEW QUESTION 245

- (Topic 4)

Security related breaches are assessed and contained through which of the following?

- A. The IT support team.
- B. A forensic analysis.
- C. Incident response
- D. Physical security team.

Answer: C

NEW QUESTION 250

- (Topic 4)

Which of the following is a symmetric encryption algorithm?

- A. 3DES
- B. MD5
- C. ECC

D. RSA

Answer: A

NEW QUESTION 251

- (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 252

- (Topic 5)

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years. This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?

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

Answer: B

NEW QUESTION 255

- (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 257

- (Topic 5)

The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called

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

Answer: A

NEW QUESTION 259

- (Topic 5)

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

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

Answer: B

NEW QUESTION 263

- (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. Baselineing of computer systems
- D. Scanning for viruses

Answer: A

NEW QUESTION 265

- (Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. The organization wants a more permanent solution to the threat to user credential compromise through phishing. What technical solution would BEST address this issue?

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

Answer: B

NEW QUESTION 268

- (Topic 5)

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

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

Answer: D

NEW QUESTION 269

- (Topic 5)

The rate of change in technology increases the importance of:

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

Answer: D

NEW QUESTION 274

- (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 276

- (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 280

- (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 282

- (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 285

- (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 287

- (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 290

- (Topic 5)

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

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

Answer: C

NEW QUESTION 293

- (Topic 5)

What are the primary reasons for the development of a business case for a security project?

- A. To estimate risk and negate liability to the company
- B. To understand the attack vectors and attack sources
- C. To communicate risk and forecast resource needs
- D. To forecast usage and cost per software licensing

Answer: C

NEW QUESTION 296

- (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 297

.....

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](#)