EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

NEW QUESTION 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
Regulatory requirements typically force organizations to implement

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

Answer: A

NEW QUESTION 3
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 4
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 5
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 6
Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 7
You have implemented a new security control. Which of the following risk strategy options have you engaged in?

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

Answer: D

NEW QUESTION 8
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 9
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 10
An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

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

Answer: A

NEW QUESTION 10
When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

A. An independent Governance, Risk and Compliance organization
B. Alignment of security goals with business goals
C. Compliance with local privacy regulations
D. Support from Legal and HR teams

Answer: B

NEW QUESTION 11
When dealing with a risk management process, asset classification is important because it will impact the overall:

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

Answer: C

NEW QUESTION 15
When managing the security architecture for your company you must consider:

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

Answer: D

NEW QUESTION 17
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 21
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 25
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. assessed by a business impact analysis.
B. protected under the information classification policy.
C. analyzed under the data ownership policy.
D. analyzed under the retention policy

Answer: D

NEW QUESTION 28
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 33
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 35
Which of the following is the MOST important benefit of an effective security governance process?

A. Reduction of liability and overall risk to the organization
B. Better vendor management
C. Reduction of security breaches
D. Senior management participation in the incident response process

Answer: A

NEW QUESTION 37
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 38
What is a difference from the list below between quantitative and qualitative Risk Assessment?

A. Quantitative risk assessments result in an exact number (in monetary terms)
B. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
C. Qualitative risk assessments map to business objectives
D. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Answer: A

NEW QUESTION 39
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 40

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 41
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 43
What is the first thing that needs to be completed in order to create a security program for your organization?

A. Risk assessment
B. Security program budget
C. Business continuity plan
D. Compliance and regulatory analysis

Answer: A

NEW QUESTION 47
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 51
Which of the following is a critical operational component of an Incident Response Program (IRP)?

A. Weekly program budget reviews to ensure the percentage of program funding remains constant.
B. Annual review of program charters, policies, procedures and organizational agreements.
C. Daily monitoring of vulnerability advisories relating to your organization’s deployed technologies.
D. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization

Answer: C

NEW QUESTION 56
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 60
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 62
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 64
Which of the following is MOST important when dealing with an Information Security Steering committee:

A. Include a mix of members from different departments and staff levels.
B. Ensure that security policies and procedures have been vetted and approved.
C. Review all past audit and compliance reports.
D. Be briefed about new trends and products at each meeting by a vendor.

Answer: C

NEW QUESTION 67
Developing effective security controls is a balance between:

A. Risk Management and Operations
B. Corporate Culture and Job Expectations
C. Operations and Regulations
D. Technology and Vendor Management

Answer: A

NEW QUESTION 72
The alerting, monitoring and life-cycle management of security related events is typically handled by the

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

Answer: A

NEW QUESTION 76
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 80
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 83
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 84
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

A. Scan a representative sample of systems
B. Perform the scans only during off-business hours
C. Decrease the vulnerabilities within the scan tool settings
D. Filter the scan output so only pertinent data is analyzed

Answer: A

NEW QUESTION 88
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 89
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 91
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 95
Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

A. Security officer
B. Data owner
C. Vulnerability engineer
D. System administrator

Answer: D

NEW QUESTION 97
When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

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

Answer: B

NEW QUESTION 102
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

A. Reduction of budget
B. Decreased security awareness
C. Improper use of information resources
D. Fines for regulatory non-compliance

Answer: D

NEW QUESTION 106
When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

A. The asset owner
B. The asset manager
C. The data custodian
D. The project manager

Answer: A

NEW QUESTION 107
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 112
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 114
You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

A. Chief Information Security Officer
B. Chief Executive Officer
C. Chief Information Officer
D. Chief Legal Counsel

Answer: B

NEW QUESTION 115
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

Explanation: Topic 2, IS Management Controls and Auditing Management

NEW QUESTION 120
Control Objectives for Information and Related Technology (COBIT) is which of the following?

A. An Information Security audit standard
B. An audit guideline for certifying secure systems and controls
C. A framework for Information Technology management and governance
D. A set of international regulations for Information Technology governance

Answer: C

NEW QUESTION 123
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 125
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 129
The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is

A. Penetration testers
B. External Audit
C. Internal Audit
D. Forensic experts

Answer: B

NEW QUESTION 132
Which of the following is a benefit of a risk-based approach to audit planning?

A. Resources are allocated to the areas of the highest concern
B. Scheduling may be performed months in advance
C. Budgets are more likely to be met by the IT audit staff
D. Staff will be exposed to a variety of technologies

Answer: A

NEW QUESTION 137
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

A. Lack of notification to the public of disclosure of confidential information.
B. Lack of periodic examination of access rights
C. Failure to notify police of an attempted intrusion
D. Lack of reporting of a successful denial of service attack on the network.

Answer: A

NEW QUESTION 142
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 147
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 149
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

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

Answer: B

NEW QUESTION 150
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 151
Which of the following illustrates an operational control process:

A. Classifying an information system as part of a risk assessment

B. Installing an appropriate fire suppression system in the data center
C. Conducting an audit of the configuration management process
D. Establishing procurement standards for cloud vendors

Answer: B

NEW QUESTION 154
You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

A. Validate that security awareness program content includes information about the potential vulnerability
B. Conduct a thorough risk assessment against the current implementation to determine system functions
C. Determine program ownership to implement compensating controls
D. Send a report to executive peers and business unit owners detailing your suspicions

Answer: B

NEW QUESTION 158
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 159
When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

A. Transfer financial resources from other critical programs
B. Take the system off line until the budget is available
C. Deploy countermeasures and compensating controls until the budget is available
D. Schedule an emergency meeting and request the funding to fix the issue

Answer: C

NEW QUESTION 163
When you develop your audit remediation plan what is the MOST important criteria?

A. To remediate half of the findings before the next audit.
B. To remediate all of the findings before the next audit.
C. To validate that the cost of the remediation is less than the risk of the finding.
D. To validate the remediation process with the auditor.

Answer: C

NEW QUESTION 168
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 171
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 175
When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

A. Daily
B. Hourly
C. Weekly

D. Monthly

Answer: A

NEW QUESTION 180
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 184
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 187
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 189
Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

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

Answer: C

NEW QUESTION 193
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 195
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 199
The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization’s

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

Answer: C

NEW QUESTION 200
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 204
An organization has implemented a change management process for all changes to the IT production environment. This change management process follows best practices and is expected to help stabilize the availability and integrity of the organization's IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process:

A. Number of change orders rejected
B. Number and length of planned outages
C. Number of unplanned outages
D. Number of change orders processed

Answer: C

NEW QUESTION 208
The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

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

Answer: C

NEW QUESTION 213
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 214
Which of the following is considered one of the most frequent failures in project management?

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

Answer: C

NEW QUESTION 215
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 217
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 218
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 222
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 225
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 227
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 229
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 234
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 238
The ultimate goal of an IT security projects is:

A. Increase stock value
B. Complete security
C. Support business requirements
D. Implement information security policies

Answer: C

NEW QUESTION 241
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 243
A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:

A. Change management
B. Business continuity planning
C. Security Incident Response
D. Thought leadership

Answer: C

NEW QUESTION 248
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 251
In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?

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

Answer: D

NEW QUESTION 255
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 256
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 258
The company decides to release the application without remediating the high-risk vulnerabilities. Which of the following is the MOST likely reason for the company to release the application?

A. The company lacks a risk management process
B. The company does not believe the security vulnerabilities to be real
C. The company has a high risk tolerance
D. The company lacks the tools to perform a vulnerability assessment

Answer: C

NEW QUESTION 259
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 261
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 265
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 267
Risk appetite is typically determined by which of the following organizational functions?

A. Security
B. Business units
C. Board of Directors
D. Audit and compliance

Answer: B

NEW QUESTION 268
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 272
The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

A. Work with the IT group and tell them to put IPS in-line and say it won't cause any network impact
B. Explain to the IT group that the IPS won't cause any network impact because it will fail open
C. Explain to the IT group that this is a business need and the IPS will fail open however, if there is a network failure the CISO will accept responsibility
D. Explain to the IT group that the IPS will fail open once in-line however it will be deployed in monitor mode for a set period of time to ensure that it doesn't block any legitimate traffic

Answer: D

NEW QUESTION 275
Which of the following best summarizes the primary goal of a security program?

A. Provide security reporting to all levels of an organization
B. Create effective security awareness to employees
C. Manage risk within the organization
D. Assure regulatory compliance

Answer: C

NEW QUESTION 279
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 282
How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?

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

Answer: D

NEW QUESTION 287
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 288
Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

A. Define the risk appetite
B. Determine budget constraints
C. Review project charters
D. Collaborate security projects

Answer: A

NEW QUESTION 292
A recommended method to document the respective roles of groups and individuals for a given process is to:

A. Develop a detailed internal organization chart
B. Develop a telephone call tree for emergency response
C. Develop an isolinear response matrix with cost benefit analysis projections
D. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart

Answer: D

NEW QUESTION 297
Which of the following can the company implement in order to avoid this type of security issue in the future?

A. Network based intrusion detection systems
B. A security training program for developers
C. A risk management process
D. A audit management process

Answer: B

NEW QUESTION 302
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 307
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 312
How often should the SSAE16 report of your vendors be reviewed?

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

Answer: C

NEW QUESTION 315
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 317
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 322
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 324
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 329
Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

A. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
B. Create separate controls for the business units based on the types of business and functions they perform
C. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
D. Provide the business units with control mandates and schedules of audits for compliance validation

Answer: C

Explanation: Topic 4, Information Security Core Competencies

NEW QUESTION 331
You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

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

Answer: D

NEW QUESTION 334
The process of identifying and classifying assets is typically included in the

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

Answer: C

NEW QUESTION 335
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 336
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 340
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 345
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

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

Answer: A

NEW QUESTION 349
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 351
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 352
What type of attack requires the least amount of technical equipment and has the highest success rate?

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

Answer: C

NEW QUESTION 354
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 356
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?

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

Answer: C

NEW QUESTION 359
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?

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

Answer: C

NEW QUESTION 364
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 369
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 372

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 377
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 379
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
The organization has already been subject to a significant amount of credit card fraud. Which of the following is the MOST likely reason for this fraud?

A. Lack of compliance to the Payment Card Industry (PCI) standards
B. Ineffective security awareness program
C. Security practices not in alignment with ISO 27000 frameworks
D. Lack of technical controls when dealing with credit card data

Answer: A

NEW QUESTION 382
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.
Using the best business practices for project management you determine that the project correct aligns with the company goals. What needs to be verified FIRST?

A. Scope of the project
B. Training of the personnel on the project
C. Timeline of the project milestones
D. Vendor for the project

Answer: A

NEW QUESTION 383
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
What is one proven method to account for common elements found within separate
regulations and/or standards?

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

Answer: D

NEW QUESTION 387
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 388
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 392
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 397
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 399
File Integrity Monitoring (FIM) is considered a

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

Answer: C

NEW QUESTION 403
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 is unsure of the information provided and orders a vendor proof of concept to validate the system's scalability. This demonstrates which of the following?

A. An approach that allows for minimum budget impact if the solution is unsuitable
B. A methodology-based approach to ensure authentication mechanism functions
C. An approach providing minimum time impact to the implementation schedules
D. A risk-based approach to determine if the solution is suitable for investment

Answer: D

NEW QUESTION 408
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 409
The new CISO was informed of all the Information Security projects that the organization has in progress. Two projects are over a year behind schedule and over budget. Using best business practices for project management you determine that the project correctly aligns with the company goals.
Which of the following needs to be performed NEXT?

A. Verify the scope of the project
B. Verify the regulatory requirements
C. Verify technical resources
D. Verify capacity constraints

Answer: C

NEW QUESTION 413
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.
You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?

A. Get approval from the board of directors
B. Screen potential vendor solutions
C. Verify that the cost of mitigation is less than the risk
D. Create a risk metrics for all unmitigated risks

Answer: C

NEW QUESTION 417
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.
Once supervisors and data owners have approved requests, information system administrators will implement

A. Technical control(s)
B. Management control(s)
C. Policy control(s)
D. Operational control(s)

Answer: A

NEW QUESTION 422
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.
Using the best business practices for project management, you determine that the project
correctly aligns with the organization goals. What should be verified next?

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

Answer: A

NEW QUESTION 424
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 425
Acceptable levels of information security risk tolerance in an organization should be determined by?

A. Corporate legal counsel
B. CISO with reference to the company goals
C. CEO and board of director
D. Corporate compliance committee

Answer: C

NEW QUESTION 430
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 433
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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 FirstTry

* 712-50 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year