



EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

NEW QUESTION 1

- (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 2

- (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 3

- (Topic 1)

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

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

Answer: C

NEW QUESTION 4

- (Topic 1)

Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 5

- (Topic 1)

Risk is defined as:

- A. Threat times vulnerability divided by control
- B. Advisory plus capability plus vulnerability
- C. Asset loss times likelihood of event
- D. Quantitative plus qualitative impact

Answer: A

NEW QUESTION 6

- (Topic 1)

Which of the following provides an audit framework?

- A. Control Objectives for IT (COBIT)
- B. Payment Card Industry-Data Security Standard (PCI-DSS)
- C. International Organization Standard (ISO) 27002
- D. National Institute of Standards and Technology (NIST) SP 800-30

Answer: :A

NEW QUESTION 7

- (Topic 1)

The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

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

Answer: B

NEW QUESTION 8

- (Topic 1)

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

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

Answer: C

NEW QUESTION 9

- (Topic 1)

What is the definition of Risk in Information Security?

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

Answer: A

NEW QUESTION 10

- (Topic 1)

Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

- A. Awareness
- B. Compliance
- C. Governance
- D. Management

Answer: C

NEW QUESTION 10

- (Topic 1)

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

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

Answer: C

NEW QUESTION 15

- (Topic 1)

Information security policies should be reviewed:

- A. by stakeholders at least annually
- B. by the CISO when new systems are brought online
- C. by the Incident Response team after an audit
- D. by internal audit semiannually

Answer: A

NEW QUESTION 16

- (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 17

- (Topic 1)

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 21

- (Topic 1)

What two methods are used to assess risk impact?

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

Answer: D

NEW QUESTION 25

- (Topic 1)

Which of the following is the MOST important benefit of an effective security governance process?

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

Answer: A

NEW QUESTION 27

- (Topic 1)

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 32

- (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 33

- (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 34

- (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 35

- (Topic 1)

An organization information security policy serves to

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

Answer: B

NEW QUESTION 36

- (Topic 1)

The FIRST step in establishing a security governance program is to?

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

Answer: :B

NEW QUESTION 41

- (Topic 1)

What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

- A. Test every three years to ensure that things work as planned
- B. Conduct periodic tabletop exercises to refine the BC plan
- C. Outsource the creation and execution of the BC plan to a third party vendor
- D. Conduct a Disaster Recovery (DR) exercise every year to test the plan

Answer: B

NEW QUESTION 42

- (Topic 1)

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

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

Answer: C

NEW QUESTION 47

- (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 49

- (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 51

- (Topic 1)

An organization's Information Security Policy is of MOST importance because

- A. it communicates management's commitment to protecting information resources
- B. it is formally acknowledged by all employees and vendors
- C. it defines a process to meet compliance requirements
- D. it establishes a framework to protect confidential information

Answer: A

NEW QUESTION 54

- (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 55

- (Topic 1)

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

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

Answer: D

NEW QUESTION 58

- (Topic 1)

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

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

Answer: :A

NEW QUESTION 59

- (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 64

- (Topic 1)

What is the MAIN reason for conflicts between Information Technology and Information Security programs?

- A. Technology governance defines technology policies and standards while security governance does not.
- B. Security governance defines technology best practices and Information Technology governance does not.
- C. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
- D. The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.

Answer: D

NEW QUESTION 65

- (Topic 1)

The PRIMARY objective for information security program development should be:

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

Answer: A

NEW QUESTION 66

- (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 71

- (Topic 1)

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

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

Answer: A

NEW QUESTION 76

- (Topic 1)

What is the main purpose of the Incident Response Team?

- A. Ensure efficient recovery and reinstate repaired systems
- B. Create effective policies detailing program activities
- C. Communicate details of information security incidents
- D. Provide current employee awareness programs

Answer: A

NEW QUESTION 80

- (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 84

- (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 87

- (Topic 1)

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

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

Answer: D

NEW QUESTION 91

- (Topic 1)

A security manager regularly checks work areas after business 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 96

- (Topic 1)

The Information Security Management program MUST protect:

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

Answer: B

NEW QUESTION 98

- (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 100

- (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 103

- (Topic 1)

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 106

- (Topic 1)

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 111

- (Topic 1)

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

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

Answer: C

NEW QUESTION 112

- (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 115

- (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 117

- (Topic 1)

A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

- A. Lack of a formal security awareness program
- B. Lack of a formal security policy governance process
- C. Lack of formal definition of roles and responsibilities
- D. Lack of a formal risk management policy

Answer: B

NEW QUESTION 121

- (Topic 1)

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 124

- (Topic 1)

A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected. Who must be informed of this incident?

- A. Internal audit
- B. The data owner
- C. All executive staff
- D. Government regulators

Answer: B

NEW QUESTION 129

- (Topic 2)

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

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

Answer: A

NEW QUESTION 134

- (Topic 2)

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 135

- (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 138

- (Topic 2)

The regular review of a firewall ruleset is considered a

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

Answer: A

NEW QUESTION 139

- (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 143

- (Topic 2)

Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

- A. Application logs
- B. File integrity monitoring
- C. SNMP traps
- D. Syslog

Answer: B

NEW QUESTION 145

- (Topic 2)

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

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

Answer: D

NEW QUESTION 149

- (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 150

- (Topic 2)

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

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

Answer: C

NEW QUESTION 155

- (Topic 2)

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

- A. Resources are allocated to the areas of the highest concern

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

Answer: A

NEW QUESTION 159

- (Topic 2)

Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?

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

Answer: D

NEW QUESTION 163

- (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 166

- (Topic 2)

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

- A. Nonlinearities in physical security performance metrics
- B. Defense in depth cost enumerated costs
- C. System hardening and patching requirements
- D. Anti-virus for mobile devices

Answer: A

NEW QUESTION 169

- (Topic 2)

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

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

Answer: B

NEW QUESTION 174

- (Topic 2)

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

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

Answer: A

NEW QUESTION 176

- (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 177

- (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 182

- (Topic 2)

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 187

- (Topic 2)

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

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

Answer: A

NEW QUESTION 188

- (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 191

- (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 195

- (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 199

- (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 203

- (Topic 2)

Which of the following activities results in change requests?

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

Answer: A

NEW QUESTION 208

- (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 213

- (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 218

- (Topic 2)

The effectiveness of an audit is measured by?

- A. The number of actionable items in the recommendations
- B. How it exposes the risk tolerance of the company
- C. How the recommendations directly support the goals of the company
- D. The number of security controls the company has in use

Answer: C

NEW QUESTION 222

- (Topic 2)

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

- A. The auditors have not followed proper auditing processes
- B. The CIO of the organization disagrees with the finding
- C. The risk tolerance of the organization permits this risk
- D. The organization has purchased cyber insurance

Answer: C

NEW QUESTION 223

- (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 224

- (Topic 2)

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

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

D. Damage control plan

Answer: :C

NEW QUESTION 226

- (Topic 2)

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

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

Answer: A

NEW QUESTION 229

- (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 234

- (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 236

- (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 240

- (Topic 2)

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 242

- (Topic 2)

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

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

Answer: C

NEW QUESTION 244

- (Topic 2)

The patching and monitoring of systems on a consistent schedule is required by?

- A. Local privacy laws
- B. Industry best practices
- C. Risk Management frameworks
- D. Audit best practices

Answer: C

NEW QUESTION 248

- (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 249

- (Topic 2)

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

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

Answer: C

NEW QUESTION 251

- (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 253

- (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 255

- (Topic 3)

Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

- A. Security administrators
- B. Security mangers
- C. Security technicians
- D. Security analysts

Answer: :B

NEW QUESTION 258

- (Topic 3)

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 259

- (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 260

- (Topic 3)

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 265

- (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 266

- (Topic 3)

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

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

Answer: D

NEW QUESTION 269

- (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 SIEM 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 272

- (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 277

- (Topic 3)

This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

- A. Scope creep
- B. Deadline extension

- C. Scope modification
- D. Deliverable expansion

Answer: A

NEW QUESTION 280

- (Topic 3)

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

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

Answer: D

NEW QUESTION 281

- (Topic 3)

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

- A. Vendors uses their own laptop and logins with same admin credentials your security team uses
- B. Vendor uses a company supplied laptop and logins using two factor authentication with same admin credentials your security team uses
- C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials
- D. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials

Answer: C

NEW QUESTION 284

- (Topic 3)

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 285

- (Topic 3)

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 288

- (Topic 3)

A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?

- A. The software license expiration is probably out of synchronization with other software licenses
- B. The project was initiated without an effort to get support from impacted business units in the organization
- C. The software is out of date and does not provide for a scalable solution across the enterprise
- D. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects

Answer: B

NEW QUESTION 290

- (Topic 3)

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

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

Answer: B

NEW QUESTION 291

- (Topic 3)

Which of the following is the MOST important component of any change management process?

- A. Scheduling
- B. Back-out procedures
- C. Outage planning
- D. Management approval

Answer: D

NEW QUESTION 294

- (Topic 3)

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

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

Answer: B

NEW QUESTION 296

- (Topic 3)

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

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

Answer: B

NEW QUESTION 299

- (Topic 3)

A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

- A. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
- B. A clear set of security policies and procedures that are more concept-based than controls-based
- C. A complete inventory of Information Technology assets including infrastructure, networks, applications and data
- D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

Answer: :D

NEW QUESTION 300

- (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 305

- (Topic 4)

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

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

Answer: D

NEW QUESTION 309

- (Topic 4)

As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.

1.Covering tracks 2.Scanning and enumeration 3.Maintaining Access 4.Reconnaissance
5.Gaining Access

- A. 4, 2, 5, 3, 1
- B. 2, 5, 3, 1, 4
- C. 4, 5, 2, 3, 1
- D. 4, 3, 5, 2, 1

Answer: A

NEW QUESTION 310

- (Topic 4)

Your organization provides open guest wireless access with no captive portals. What can you do to assist with law enforcement investigations if one of your guests is suspected of committing an illegal act using your network?

- A. Configure logging on each access point
- B. Install a firewall software on each wireless access point.
- C. Provide IP and MAC address
- D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.

Answer: :C

NEW QUESTION 315

- (Topic 4)

Which of the following is the MAIN security concern for public cloud computing?

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

Answer: A

NEW QUESTION 319

- (Topic 4)

Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the incident handling process will utilize the signature to resolve this incident?

- A. Containment
- B. Recovery
- C. Identification
- D. Eradication

Answer: D

NEW QUESTION 321

- (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 326

- (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 329

- (Topic 4)

While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

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

Answer: B

NEW QUESTION 334

- (Topic 4)

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

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

Answer: A

NEW QUESTION 338

- (Topic 4)

An anonymity network is a series of?

- A. Covert government networks
- B. War driving maps
- C. Government networks in Tora
- D. Virtual network tunnels

Answer: D

NEW QUESTION 339

- (Topic 4)

Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

- A. Trusted and untrusted networks
- B. Type of authentication
- C. Storage encryption
- D. Log retention

Answer: A

NEW QUESTION 342

- (Topic 4)

The process for identifying, collecting, and producing digital information in support of legal proceedings is called

- A. chain of custody.
- B. electronic discovery.
- C. evidence tampering.
- D. electronic review.

Answer: B

NEW QUESTION 344

- (Topic 4)

Which of the following statements about Encapsulating Security Payload (ESP) is true?

- A. It is an IPSec protocol.
- B. It is a text-based communication protocol.
- C. It uses TCP port 22 as the default port and operates at the application layer.
- D. It uses UDP port 22

Answer: A

NEW QUESTION 346

- (Topic 4)

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

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

Answer: C

NEW QUESTION 351

- (Topic 4)

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

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

Answer: A

NEW QUESTION 352

- (Topic 5)

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

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

Answer: C

NEW QUESTION 357

- (Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. What type of control is being implemented by supervisors and data owners?

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

Answer: B

NEW QUESTION 359

- (Topic 5)

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

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

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

Answer: C

NEW QUESTION 362

- (Topic 5)

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

The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization. From an organizational perspective, which of the following is the LIKELY reason for this?

- A. The CISO does not report directly to the CEO of the organization
- B. The CISO reports to the IT organization
- C. The CISO has not implemented a policy management framework
- D. The CISO has not implemented a security awareness program

Answer: B

NEW QUESTION 367

- (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 368

- (Topic 5)

What is the BEST reason for having a formal request for proposal process?

- A. Creates a timeline for purchasing and budgeting
- B. Allows small companies to compete with larger companies
- C. Clearly identifies risks and benefits before funding is spent
- D. Informs suppliers a company is going to make a purchase

Answer: C

NEW QUESTION 369

- (Topic 5)

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

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

Answer: B

NEW QUESTION 374

- (Topic 5)

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 correctly aligns with the company goals and the scope of the project is correct. What is the NEXT step?

- A. Review time schedules
- B. Verify budget
- C. Verify resources
- D. Verify constraints

Answer: C

NEW QUESTION 376

- (Topic 5)

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

The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning. Which of the following is the MOST logical next step?

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

Answer: C

NEW QUESTION 379

- (Topic 5)

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

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

Answer: C

NEW QUESTION 382

- (Topic 5)

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

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

Answer: B

NEW QUESTION 386

- (Topic 5)

Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.

To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

- A. Business Impact Analysis
- B. Business Continuity plan
- C. Security roadmap
- D. Annual report to shareholders

Answer: A

NEW QUESTION 391

- (Topic 5)

What is the primary reason for performing vendor management?

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

Answer: A

NEW QUESTION 395

- (Topic 5)

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

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

Answer: B

NEW QUESTION 397

- (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. 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 401

- (Topic 5)

Human resource planning for security professionals in your organization is a:

- A. Simple and easy task because the threats are getting easier to find and correct.
- B. Training requirement that is met through once every year user training.
- C. Training requirement that is on-going and always changing.
- D. Not needed because automation and anti-virus software has eliminated the threats.

Answer: C

NEW QUESTION 402

- (Topic 5)

When analyzing and forecasting an operating expense budget what are not included?

- A. Software and hardware license fees
- B. Utilities and power costs
- C. Network connectivity costs
- D. New datacenter to operate from

Answer: D

NEW QUESTION 407

- (Topic 5)

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

Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

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

Answer: A

NEW QUESTION 409

- (Topic 5)

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

- A. Create timelines for mitigation
- B. Develop a cost-benefit analysis

- C. Calculate annual loss expectancy
- D. Create a detailed technical executive summary

Answer: B

NEW QUESTION 414

- (Topic 5)

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

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

Answer: B

NEW QUESTION 419

- (Topic 5)

The formal certification and accreditation process has four primary steps, what are they?

- A. Evaluating, describing, testing and authorizing
- B. Evaluating, purchasing, testing, authorizing
- C. Auditing, documenting, verifying, certifying
- D. Discovery, testing, authorizing, certifying

Answer: A

NEW QUESTION 424

- (Topic 5)

Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the “real workers.”

What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

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

Answer: B

NEW QUESTION 425

- (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 429

- (Topic 5)

File Integrity Monitoring (FIM) is considered a

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

Answer: C

NEW QUESTION 433

- (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 435

- (Topic 5)

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 439

- (Topic 5)

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

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

Answer: C

NEW QUESTION 443

- (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. 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 446

- (Topic 5)

The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

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

Answer: B

NEW QUESTION 451

- (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 453

- (Topic 5)

Acceptable levels of information security risk tolerance in an organization should be determined by?

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

Answer: C

NEW QUESTION 455

.....

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](#)