EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)

NEW QUESTION 1
- (Exam Topic 6)
Devising controls for information security is a balance between?

A. Governance and compliance
B. Auditing and security
C. Budget and risk tolerance
D. Threats and vulnerabilities

Answer: C

Explanation:
Reference: https://www.cybok.org/media/downloads/cybok_version_1.0.pdf

NEW QUESTION 2
- (Exam Topic 6)
The primary responsibility for assigning entitlements to a network share lies with which role?

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

Answer: B

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

NEW QUESTION 3
- (Exam Topic 6)
A Security Operations Manager is finding it difficult to maintain adequate staff levels to monitor security operations during off-hours. To reduce the impact of staff shortages and increase coverage during off-hours, the SecOps manager is considering outsourcing off-hour coverage.
What Security Operations Center (SOC) model does this BEST describe?

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

Answer: A

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

NEW QUESTION 4
- (Exam Topic 6)
During a cyber incident, which non-security personnel might be needed to assist the security team?

A. Threat analyst, IT auditor, forensic analyst
B. Network engineer, help desk technician, system administrator
C. CIO, CFO, CSO
D. Financial analyst, payroll clerk, HR manager

Answer: A

NEW QUESTION 5
- (Exam Topic 6)
Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person’s eye. However, authorization failures can occur with individuals who have?

A. Glaucoma or cataracts
B. Two different colored eyes (heterochromia iridium)
C. Contact lens
D. Malaria

Answer: A

NEW QUESTION 6
- (Exam Topic 6)
Which of the following strategies provides the BEST response to a ransomware attack?

A. Real-time off-site replication
B. Daily incremental backup
C. Daily full backup

D. Daily differential backup

Answer: B

NEW QUESTION 7
- (Exam Topic 6)
The Board of Directors of a publicly-traded company is concerned about the security implications of a strategic project that will migrate 50% of the organization's information technology assets to the cloud. They have requested a briefing on the project plan and a progress report of the security stream of the project. As the CISO, you have been tasked with preparing the report for the Chief Executive Officer to present.
Using the Earned Value Management (EVM), what does a Cost Variance (CV) of -1,200 mean?

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

Answer: A

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

NEW QUESTION 8
- (Exam Topic 6)
What is a Statement of Objectives (SOA)?

A. A section of a contract that defines tasks to be performed under said contract
B. An outline of what the military will do during war
C. A document that outlines specific desired outcomes as part of a request for proposal
D. Business guidance provided by the CEO

Answer: A

NEW QUESTION 9
- (Exam Topic 6)
When managing a project, the MOST important activity in managing the expectations of stakeholders is:

A. To force stakeholders to commit ample resources to support the project
B. To facilitate proper communication regarding outcomes
C. To assure stakeholders commit to the project start and end dates in writing
D. To finalize detailed scope of the project at project initiation

Answer: B

Explanation:
Reference:
https://www.greycampus.com/blog/project-management/stakeholder-management-what-is-it-and-why-is-it-so-im

NEW QUESTION 10
- (Exam Topic 6)
XYZ is a publicly-traded software development company.
Who is ultimately accountable to the shareholders in the event of a cybersecurity breach?

A. Chief Financial Officer (CFO)
B. Chief Software Architect (CIO)
C. CISO
D. Chief Executive Officer (CEO)

Answer: C

Explanation:
Reference: https://www.eccouncil.org/information-security-management/

NEW QUESTION 10
- (Exam Topic 6)
Which of the following is the MOST effective method to counter phishing attacks?

A. User awareness and training
B. Host based Intrusion Detection System (IPS)
C. Acceptable use guide signed by all system users
D. Antispam solution

Answer: A

Explanation:
Reference: https://aware.eccouncil.org/4-best-ways-to-stop-phishing-with-security-awareness.html

NEW QUESTION 11
- (Exam Topic 6)
ABC Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame. You would like to implement key performance indicators to mitigate the risk.
Which metric would meet the requirement?

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

Answer: C

NEW QUESTION 16
- (Exam Topic 2)
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 21
- (Exam Topic 2)
When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

A. ISO 27001
B. PRINCE2
C. ISO 27004
D. ITILv3

Answer: C

NEW QUESTION 25
- (Exam Topic 2)
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

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

Answer: B

NEW QUESTION 28
- (Exam Topic 2)
Which of the following activities is the MAIN purpose of the risk assessment process?

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

Answer: D

NEW QUESTION 33
- (Exam Topic 2)
The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization's

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

Answer: C

NEW QUESTION 36
- (Exam Topic 2)
A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.

C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
D. If the findings do not impact regulatory compliance, review current security controls.

Answer: C

NEW QUESTION 40
- (Exam 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 43
- (Exam Topic 2)
Which of the following is a fundamental component of an audit record?

A. Date and time of the event
B. Failure of the event
C. Originating IP-Address
D. Authentication type

Answer: A

NEW QUESTION 45
- (Exam Topic 2)
Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

A. It allows executives to more effectively monitor IT implementation costs
B. Implementation of it eases an organization's auditing and compliance burden
C. Information Security (IS) procedures often require augmentation with other standards
D. It provides for a consistent and repeatable staffing model for technology organizations

Answer: B

NEW QUESTION 48
- (Exam Topic 2)
To have accurate and effective information security policies how often should the CISO review the organization policies?

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

Answer: D

NEW QUESTION 53
- (Exam Topic 2)
Which of the following are necessary to formulate responses to external audit findings?

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

Answer: C

NEW QUESTION 56
- (Exam Topic 2)
Creating a secondary authentication process for network access would be an example of?

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

Answer: C

NEW QUESTION 58
- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 60
- (Exam Topic 1)
An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?

A. Determine the risk tolerance
B. Perform an asset classification
C. Create an architecture gap analysis
D. Analyze existing controls on systems

Answer: B

NEW QUESTION 65
- (Exam Topic 1)
Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

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

Answer: C

NEW QUESTION 67
- (Exam 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 70
- (Exam 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 71
- (Exam Topic 1)
One of the MAIN goals of a Business Continuity Plan is to

A. Ensure all infrastructure and applications are available in the event of a disaster
B. Allow all technical first-responders to understand their roles in the event of a disaster
C. Provide step by step plans to recover business processes in the event of a disaster
D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer: C

NEW QUESTION 76
- (Exam 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 81
- (Exam Topic 1)
A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

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

Answer: C

NEW QUESTION 82
- (Exam 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 84
- (Exam Topic 1)
Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

A. Threat
B. Vulnerability
C. Attack vector
D. Exploitation

Answer: B

NEW QUESTION 88
- (Exam Topic 1)
After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

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

Answer: D

NEW QUESTION 90
- (Exam 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 94
- (Exam Topic 1)
What is the definition of Risk in Information Security?

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

Answer: A

NEW QUESTION 98
- (Exam Topic 1)
The PRIMARY objective for information security program development should be:

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

Answer: A

NEW QUESTION 99
- (Exam Topic 1)
Which of the following is the MOST important for a CISO to understand when identifying threats?

A. How vulnerabilities can potentially be exploited in systems that impact the organization
B. How the security operations team will behave to reported incidents
C. How the firewall and other security devices are configured to prevent attacks
D. How the incident management team prepares to handle an attack

Answer: A

NEW QUESTION 102
- (Exam 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 105
- (Exam Topic 1)
Which of the following most commonly falls within the scope of an information security governance steering committee?

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

Answer: D

NEW QUESTION 107
- (Exam Topic 1)
The PRIMARY objective of security awareness is to:

A. Ensure that security policies are read.
B. Encourage security-conscious employee behavior.
C. Meet legal and regulatory requirements.
D. Put employees on notice in case follow-up action for noncompliance is necessary

Answer: B

NEW QUESTION 108
- (Exam Topic 1)
What is the BEST way to achieve on-going compliance monitoring in an organization?

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

Answer: C

NEW QUESTION 109
- (Exam Topic 1)
Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 110
- (Exam Topic 1)
You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

A. Controlled mitigation effort
B. Risk impact comparison
C. Relative likelihood of event

D. Comparative threat analysis

Answer: C

NEW QUESTION 111
- (Exam 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 114
- (Exam 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 119
- (Exam Topic 1)
An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

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

Answer: D

NEW QUESTION 123
- (Exam 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 128
- (Exam Topic 1)
Which of the following is considered the MOST effective tool against social engineering?

A. Anti-phishing tools
B. Anti-malware tools
C. Effective Security Vulnerability Management Program
D. Effective Security awareness program

Answer: D

NEW QUESTION 129
- (Exam Topic 1)
When dealing with a risk management process, asset classification is important because it will impact the overall:

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

Answer: C

NEW QUESTION 134
- (Exam Topic 1)
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 137
- (Exam Topic 1)
A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?

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

Answer: C

NEW QUESTION 138
- (Exam Topic 1)
According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

A. Identify threats, risks, impacts and vulnerabilities
B. Decide how to manage risk
C. Define the budget of the Information Security Management System
D. Define Information Security Policy

Answer: D

NEW QUESTION 142
- (Exam Topic 1)
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

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

Answer: B

NEW QUESTION 144
- (Exam Topic 1)
Credit card information, medical data, and government records are all examples of:

A. Confidential/Protected Information
B. Bodily Information
C. Territorial Information
D. Communications Information

Answer: A

NEW QUESTION 146
- (Exam Topic 1)
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer: A

NEW QUESTION 151
- (Exam Topic 1)
An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System. Which of the following international standards can BEST assist this organization?

A. International Organization for Standardizations – 27004 (ISO-27004)
B. Payment Card Industry Data Security Standards (PCI-DSS)
C. Control Objectives for Information Technology (COBIT)
D. International Organization for Standardizations – 27005 (ISO-27005)

Answer: A

NEW QUESTION 155
- (Exam Topic 1)
When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

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

Answer: B

NEW QUESTION 160
- (Exam 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 164
- (Exam Topic 1)
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

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

Answer: C

NEW QUESTION 168
- (Exam Topic 1)
The success of the Chief Information Security Officer is MOST dependent upon:

A. favorable audit findings
B. following the recommendations of consultants and contractors
C. development of relationships with organization executives
D. raising awareness of security issues with end users

Answer: C

NEW QUESTION 172
- (Exam 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 177
- (Exam Topic 1)
Who in the organization determines access to information?

A. Legal department
B. Compliance officer
C. Data Owner
D. Information security officer

Answer: C

NEW QUESTION 178
- (Exam Topic 1)
Which of the following are the MOST important factors for proactively determining system vulnerabilities?

A. Subscribe to vendor mailing list to get notification of system vulnerabilities
B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
D. Conduct security testing, vulnerability scanning, and penetration testing

Answer:

D

NEW QUESTION 182
- (Exam Topic 1)
In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

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

Answer: B

NEW QUESTION 186
- (Exam Topic 1)
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

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

Answer: A

NEW QUESTION 188
- (Exam 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 190
- (Exam Topic 6)
What are the common data hiding techniques used by criminals?

A. Unallocated space and masking
B. Website defacement and log manipulation
C. Disabled Logging and admin elevation
D. Encryption, Steganography, and Changing Metadata/Timestamps

Answer: D

Explanation:
Reference: https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/

NEW QUESTION 193
- (Exam Topic 6)
You have been promoted to the CISO of a big-box retail store chain reporting to the Chief Information Officer (CIO). The CIO's first mandate to you is to develop a cybersecurity compliance framework that will meet all the store's compliance requirements.
Which of the following compliance standard is the MOST important to the organization?

A. The Federal Risk and Authorization Management Program (FedRAMP)
B. ISO 27002
C. NIST Cybersecurity Framework
D. Payment Card Industry (PCI) Data Security Standard (DSS)

Answer: D

Explanation:
Reference:
https://searchcompliance.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

NEW QUESTION 198
- (Exam Topic 6)
You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans.
Which control is MOST important to protect AI products?

A. Hash datasets
B. Sanitize datasets
C. Delete datasets
D. Encrypt datasets

Answer: D

NEW QUESTION 199
- (Exam Topic 6)
You have been hired as the Information System Security Officer (ISSO) for a US federal government agency. Your role is to ensure the security posture of the system is maintained. One of your tasks is to develop and maintain the system security plan (SSP) and supporting documentation.
Which of the following is NOT documented in the SSP?

A. The controls in place to secure the system
B. Name of the connected system
C. The results of a third-party audits and recommendations
D. Type of information used in the system

Answer: C

Explanation:
Reference:
https://www.govinfo.gov/content/pkg/GOVPUB-C13-63e84ab7af43b36228f10e4f0b5f8c38/pdf/GOVPUB-C13- (65)

NEW QUESTION 200
- (Exam Topic 6)
Who should be involved in the development of an internal campaign to address email phishing?

A. Business unit leaders, CIO, CEO
B. Business Unite Leaders, CISO, CIO and CEO
C. All employees
D. CFO, CEO, CIO

Answer: B

NEW QUESTION 202
- (Exam Topic 6)
What is an approach to estimating the strengths and weaknesses of alternatives used to determine options, which provide the BEST approach to achieving benefits while preserving savings called?

A. Business Impact Analysis
B. Economic Impact analysis
C. Return on Investment
D. Cost-benefit analysis

Answer: D

Explanation:
Reference: https://artsandculture.google.com/entity/cost%E2%80%93benefit-analysis/m020w0x?hl=en

NEW QUESTION 205
- (Exam Topic 6)
When evaluating a Managed Security Services Provider (MSSP), which service(s) is/are most important:

A. Patch management
B. Network monitoring
C. Ability to provide security services tailored to the business' needs
D. 24/7 tollfree number

Answer: C

Explanation:
Reference: https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps

NEW QUESTION 210
- (Exam Topic 6)
As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity.
The performance quality audit activity is done in what project management process group?

A. Executing
B. Controlling
C. Planning
D. Closing

Answer: A

Explanation:
Reference:
https://blog.masterofproject.com/executing-process-group-project-management/#:~:text=Executing%20Process

NEW QUESTION 215
- (Exam Topic 6)
What is a key policy that should be part of the information security plan?

A. Account management policy
B. Training policy
C. Acceptable Use policy
D. Remote Access policy

Answer: C

Explanation:
Reference: https://www.exabeam.com/information-security/information-security-policy/

NEW QUESTION 220
- (Exam Topic 6)
A CISO must conduct risk assessments using a method where the Chief Financial Officer (CFO) receives impact data in financial terms to use as input to select the proper level of coverage in a new cybersecurity insurance policy.
What is the MOST effective method of risk analysis to provide the CFO with the information required?

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

Answer: D

NEW QUESTION 221
- (Exam Topic 6)
As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand.
Which is the BEST type of risk that defines this event?

A. Compliance Risk
B. Reputation Risk
C. Operational Risk
D. Strategic Risk

Answer: B

NEW QUESTION 224
- (Exam Topic 5)
Using the Transport Layer Security (TLS) protocol enables a client in a network to be:

A. Provided with a digital signature
B. Assured of the server's identity
C. Identified by a network
D. Registered by the server

Answer: B

Explanation:
Reference: https://ukdiss.com/examples/tls.php

NEW QUESTION 229
- (Exam Topic 5)
Which of the following is true regarding expenditures?

A. Capital expenditures are never taxable
B. Operating expenditures are for acquiring assets, capital expenditures are for support costs of that asset
C. Capital expenditures are used to define depreciation tables of intangible assets
D. Capital expenditures are for acquiring assets, whereas operating expenditures are for support costs of that asset

Answer: D

NEW QUESTION 234
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda. From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?

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

Answer: B

NEW QUESTION 238
- (Exam Topic 5)
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
When multiple regulations or standards apply to your industry you should set controls to meet the:

A. Easiest regulation or standard to implement
B. Stricter regulation or standard
C. Most complex standard to implement
D. Recommendations of your Legal Staff

Answer: C

NEW QUESTION 241
- (Exam Topic 5)
What are the three stages of an identity and access management system?

A. Authentication, Authorize, Validation
B. Provision, Administration, Enforcement
C. Administration, Validation, Protect
D. Provision, Administration, Authentication

Answer: A

Explanation:
Reference: https://digitalguardian.com/blog/what-identity-and-access-management-iam

NEW QUESTION 246
- (Exam Topic 5)
What are the three hierarchically related aspects of strategic planning and in which order should they be done?

A. 1) Information technology strategic planning, 2) Enterprise strategic planning, 3) Cybersecurity orinformation security strategic planning
B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3)Informationtechnology strategic planning
C. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning
D. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3)Information technology strategic planning

Answer: D

NEW QUESTION 248
- (Exam Topic 5)
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

A. Video surveillance
B. Mantrap
C. Bollards
D. Fence

Answer: D

NEW QUESTION 253
- (Exam Topic 5)
As the CISO you need to write the IT security strategic plan. Which of the following is the MOST important to review before you start writing the plan?

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

Answer: B

NEW QUESTION 256
- (Exam Topic 5)
The rate of change in technology increases the importance of:

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

Answer: D

NEW QUESTION 259
- (Exam Topic 5)
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.

Which of the following would be the FIRST step when addressing Information Security formally and consistently in this organization?

A. Contract a third party to perform a security risk assessment
B. Define formal roles and responsibilities for Internal audit functions
C. Define formal roles and responsibilities for Information Security
D. Create an executive security steering committee

Answer: C

NEW QUESTION 262
- (Exam Topic 5)
A CISO wants to change the defense strategy to ward off attackers. To accomplish this the CISO is looking to a strategy where attackers are lured into a zone of a safe network where attackers can be monitored, controlled, quarantined, or eradicated.

A. Moderate investment
B. Passive monitoring
C. Integrated security controls
D. Dynamic deception

Answer: D

NEW QUESTION 263
- (Exam Topic 5)
When analyzing and forecasting a capital expense budget what are not included?

A. Network connectivity costs
B. New datacenter to operate from
C. Upgrade of mainframe
D. Purchase of new mobile devices to improve operations

Answer: A

NEW QUESTION 266
- (Exam Topic 5)
An organization has a number of Local Area Networks (LANs) linked to form a single Wide Area Network (WAN). Which of the following would BEST ensure network continuity?

A. Third-party emergency repair contract
B. Pre-built servers and routers
C. Permanent alternative routing
D. Full off-site backup of every server

Answer: C

NEW QUESTION 270
- (Exam Topic 5)
Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

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

Answer: A

NEW QUESTION 274
- (Exam Topic 5)
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.
Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

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

Answer: C

NEW QUESTION 275
- (Exam Topic 5)
Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

A. Segmentation controls.
B. Shadow applications.
C. Deception technology.
D. Vulnerability management.

Answer: B

NEW QUESTION 280
- (Exam Topic 5)
During the last decade, what trend has caused the MOST serious issues in relation to physical security?

A. Data is more portable due to the increased use of smartphones and tablets
B. The move from centralized computing to decentralized computing
C. Camera systems have become more economical and expanded in their use
D. The internet of Things allows easy compromise of cloud-based systems

Answer: A

NEW QUESTION 284
- (Exam Topic 5)
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
Which of the following frameworks and standards will BEST fit the organization as a baseline for their security program?

A. NIST and Privacy Regulations
B. ISO 27000 and Payment Card Industry Data Security Standards
C. NIST and data breach notification laws
D. ISO 27000 and Human resources best practices

Answer: B

NEW QUESTION 286
- (Exam Topic 5)
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.
This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?

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

Answer: B

NEW QUESTION 287
- (Exam Topic 5)
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
What is one proven method to account for common elements found within separate regulations and/or standards?

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

Answer: D

NEW QUESTION 290
- (Exam Topic 5)
SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.
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 293
- (Exam Topic 5)
The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

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

Answer: C

NEW QUESTION 296
- (Exam Topic 5)
SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.
After determining the audit findings are accurate, which of the following is the MOST logical next activity?

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

Answer: A

NEW QUESTION 299
- (Exam Topic 5)
The formal certification and accreditation process has four primary steps, what are they?

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

Answer: A

NEW QUESTION 304
- (Exam Topic 5)
John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can John do in this instance?

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

Answer: D

NEW QUESTION 308
- (Exam Topic 5)
The primary purpose of a risk register is to:

A. Maintain a log of discovered risks
B. Track individual risk assessments
C. Develop plans for mitigating identified risks
D. Coordinate the timing of scheduled risk assessments

Answer: A

Explanation:
Reference: https://sitemate.com/us/resources/articles/safety/purpose-of-a-risk-register/

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

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

Answer: A

NEW QUESTION 313
- (Exam Topic 5)
During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

A. The budget is in a temporary state of imbalance
B. The budget is operating at a deficit
C. She can realign the budget through moderate capital expense (CAPEX) allocation
D. She has a surplus of operational expenses (OPEX)

Answer: A

NEW QUESTION 316

- (Exam Topic 5)
A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

A. Poorly configured firewalls
B. Malware
C. Advanced Persistent Threat (APT)
D. An insider

Answer: D

NEW QUESTION 318
- (Exam Topic 5)
SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs.
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 320
- (Exam Topic 5)
A newly-hired CISO needs to understand the organization's financial management standards for business units and operations. Which of the following would be the best source of this information?

A. The internal accounting department
B. The Chief Financial Officer (CFO)
C. The external financial audit service
D. The managers of the accounts payables and accounts receivables teams

Answer: D

NEW QUESTION 323
- (Exam Topic 5)
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years. 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 328
- (Exam Topic 5)
As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

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

Answer: D

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

NEW QUESTION 331
- (Exam Topic 5)
When project costs continually increase throughout implementation due to large or rapid changes in customer or user requirements, this is commonly known as:

A. Cost/benefit adjustments
B. Scope creep
C. Prototype issues
D. Expectations management

Answer: B

Explanation:
Reference:

http://www.umsl.edu/~sauterv/analysis/6840_f03_papers/gurlen/

NEW QUESTION 333
- (Exam 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 335
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?

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

Answer: C

NEW QUESTION 338
- (Exam Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

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

Answer: A

NEW QUESTION 339
- (Exam Topic 5)
What is one key difference between Capital expenditures and Operating expenditures?

A. Operating expense cannot be written off while Capital expense can
B. Operating expenses can be depreciated over time and Capital expenses cannot
C. Capital expenses cannot include salaries and Operating expenses can
D. Capital expenditures allow for the cost to be depreciated over time and Operating does not

Answer: C

NEW QUESTION 344
- (Exam Topic 5)
Acceptable levels of information security risk tolerance in an organization should be determined by?

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

Answer: C

NEW QUESTION 349
- (Exam 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 351
- (Exam Topic 5)
Which of the following is an accurate description of a balance sheet?

A. The percentage of earnings that are retained by the organization for reinvestment in the business
B. The details of expenses and revenue over a long period of time
C. A summarized statement of all assets and liabilities at a specific point in time
D. A review of regulations and requirements impacting the business from a financial perspective

Answer: C

NEW QUESTION 355
- (Exam Topic 5)
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.
You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

A. Conduct background checks on individuals before hiring them
B. Develop an Information Security Awareness program
C. Monitor employee browsing and surfing habits
D. Set your firewall permissions aggressively and monitor logs regularly.

Answer: A

NEW QUESTION 356
- (Exam Topic 5)
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Post a sign that states, “no tailgating” next to the special card reader adjacent to the secure door
B. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
C. Educate and enforce physical security policies of the company to all the employees on a regular basis
D. Setup a mock video camera next to the special card reader adjacent to the secure door

Answer: C

NEW QUESTION 358
- (Exam Topic 5)
If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization. How would you prevent such type of attacks?

A. Conduct thorough background checks before you engage them
B. Hire the people through third-party job agencies who will vet them for you
C. Investigate their social networking profiles
D. It is impossible to block these attacks

Answer: A

NEW QUESTION 362
- (Exam Topic 5)
Which type of physical security control scan a person’s external features through a digital video camera before granting access to a restricted area?

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

Answer: C

NEW QUESTION 366
- (Exam Topic 5)
Which of the following terms is used to describe countermeasures implemented to minimize risks to physical property, information, and computing systems?

A. Security frameworks
B. Security policies
C. Security awareness
D. Security controls

Answer: D

Explanation:
Reference: https://www.ibm.com/cloud/learn/security-controls

NEW QUESTION 368
- (Exam Topic 5)
Which of the following is the MOST important reason for performing assessments of the security portfolio?

A. To assure that the portfolio is aligned to the needs of the broader organization
B. To create executive support of the portfolio
C. To discover new technologies and processes for implementation within the portfolio
D. To provide independent 3rd party reviews of security effectiveness

Answer: A

NEW QUESTION 372
- (Exam Topic 5)
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.
You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?

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

Answer: C

NEW QUESTION 377
- (Exam 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 381
- (Exam 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 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 385
- (Exam Topic 5)
Which of the following is the MOST logical method of deploying security controls within an organization?

A. Obtain funding for all desired controls and then create project plans for implementation
B. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult andcostly controls
C. Apply the least costly controls to demonstrate positive program activity
D. Obtain business unit buy-in through close communication and coordination

Answer: B

NEW QUESTION 386
- (Exam Topic 5)
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.
When formulating the remediation plan, what is a required input?

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

Answer: B

NEW QUESTION 387
- (Exam Topic 5)
What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

A. Internal Audit
B. Corporate governance
C. Risk Oversight
D. Key Performance Indicators

Answer: B

Explanation:
Reference: https://www.igi-global.com/dictionary/corporate-governance/5957

NEW QUESTION 390
- (Exam Topic 5)
Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

A. Rights collision
B. Excessive privileges
C. Privilege creep
D. Least privileges

Answer: B

NEW QUESTION 391
- (Exam Topic 5)
Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?

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

Answer: C

NEW QUESTION 393
- (Exam Topic 5)
The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called

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

Answer: A

NEW QUESTION 398
- (Exam Topic 5)
Which of the following is an accurate statement regarding capital expenses?

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

Answer: A

NEW QUESTION 402
- (Exam Topic 5)
Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

A. Reviewing system administrator logs
B. Auditing configuration templates
C. Checking vendor product releases
D. Performing system scans

Answer: D

NEW QUESTION 403
- (Exam Topic 5)
Which technology can provide a computing environment without requiring a dedicated hardware backend?

A. Mainframe server
B. Virtual Desktop
C. Thin client
D. Virtual Local Area Network

Answer: B

NEW QUESTION 407
- (Exam Topic 5)
Which of the following would negatively impact a log analysis of a multinational organization?

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

Answer: D

NEW QUESTION 412
- (Exam Topic 4)
Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?

A. In-line hardware keyloggers don’t require physical access
B. In-line hardware keyloggers don’t comply to industry regulations
C. In-line hardware keyloggers are undetectable by software
D. In-line hardware keyloggers are relatively inexpensive

Answer: C

NEW QUESTION 415
- (Exam Topic 5)
As the Chief Information Security Officer, you are performing an assessment of security posture to understand what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows to detect and actively stop vulnerability exploits and attacks?

A. Gigamon
B. Intrusion Prevention System
C. Port Security
D. Anti-virus

Answer: B

Explanation:
Reference: https://searchsecurity.techtarget.com/definition/intrusion-prevention

NEW QUESTION 418
- (Exam 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 419
- (Exam 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 422
- (Exam Topic 4)
The process of creating a system which divides documents based on their security level to manage access to private data is known as

A. security coding
B. data security system
C. data classification
D. privacy protection

Answer: C

NEW QUESTION 426
- (Exam 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 427
- (Exam Topic 4)
Physical security measures typically include which of the following components?

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

Answer: A

NEW QUESTION 430
- (Exam Topic 4)
The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?

A. Well established and defined digital forensics process
B. Establishing Enterprise-owned Botnets for preemptive attacks
C. Be able to retaliate under the framework of Active Defense
D. Collaboration with law enforcement

Answer: A

NEW QUESTION 433
- (Exam Topic 4)
A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?

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

Answer: A

NEW QUESTION 435
- (Exam 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 440
- (Exam Topic 4)
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

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

Answer: A

NEW QUESTION 442
- (Exam 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 447
- (Exam Topic 4)
SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

A. ‘ o 1=1 -
B. /../../../../
C. “DROPTABLE USERNAME”
D. NOPS

Answer: A

NEW QUESTION 449
- (Exam Topic 4)
Which wireless encryption technology makes use of temporal keys?

A. Wireless Application Protocol (WAP)
B. Wifi Protected Access version 2 (WPA2)
C. Wireless Equivalence Protocol (WEP)
D. Extensible Authentication Protocol (EAP)

Answer: B

NEW QUESTION 451
- (Exam Topic 4)
What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

A. Traffic Analysis
B. Deep-Packet inspection
C. Packet sampling
D. Heuristic analysis

Answer: B

NEW QUESTION 452
- (Exam Topic 4)
What is the FIRST step in developing the vulnerability management program?

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

Answer: A

NEW QUESTION 454
- (Exam Topic 4)
You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

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

Answer: D

NEW QUESTION 455
- (Exam Topic 3)
An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in 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 457
- (Exam Topic 3)
You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

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

Answer: B

NEW QUESTION 462
- (Exam Topic 3)
This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

A. Scope creep
B. Deadline extension
C. Scope modification
D. Deliverable expansion

Answer: A

NEW QUESTION 463
- (Exam Topic 3)
As the CISO for your company you are accountable for the protection of information resources commensurate with:

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

Answer: D

NEW QUESTION 466
- (Exam Topic 3)
Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

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

Answer: C

NEW QUESTION 467
- (Exam Topic 3)
The organization does not have the time to remediate the vulnerability; however it is critical to release the application. Which of the following needs to be further evaluated to help mitigate the risks?

A. Provide developer security training
B. Deploy Intrusion Detection Systems
C. Provide security testing tools
D. Implement Compensating Controls

Answer: D

NEW QUESTION 469
- (Exam Topic 3)
When is an application security development project complete?

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

Answer: A

NEW QUESTION 472
- (Exam Topic 3)
The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

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

Answer: D

NEW QUESTION 475
- (Exam Topic 3)
The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any

additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong? (choose the BEST answer):

A. Failed to identify all stakeholders and their needs
B. Deployed the encryption solution in an inadequate manner
C. Used 1024 bit encryption when 256 bit would have sufficed
D. Used hardware encryption instead of software encryption

Answer: A

NEW QUESTION 477
- (Exam Topic 3)
Your incident response plan should include which of the following?

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

Answer: C

NEW QUESTION 480
- (Exam Topic 3)
When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

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

Answer: C

NEW QUESTION 482
- (Exam Topic 3)
Which of the following represents the best method of ensuring business unit alignment with security program requirements?

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

Answer: C

NEW QUESTION 485
- (Exam Topic 3)
In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

A. Distance learning/Web seminars
B. Formal Class
C. One-One Training
D. Self –Study (noncomputerized)

Answer: D

NEW QUESTION 489
- (Exam Topic 3)
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

NEW QUESTION 490
- (Exam 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 493
- (Exam 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 496
- (Exam Topic 3)
What oversight should the information security team have in the change management process for application security?

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

Answer: C

NEW QUESTION 499
- (Exam Topic 3)
A stakeholder is a person or group:

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

Answer: A

NEW QUESTION 501
- (Exam 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 504
- (Exam Topic 3)
Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement. What type of risk tolerance is Acme exhibiting? (choose the BEST answer):

A. low risk-tolerance
B. high risk-tolerance
C. moderate risk-tolerance
D. medium-high risk-tolerance

Answer: A

NEW QUESTION 509
- (Exam Topic 3)
Which of the following information may be found in table top exercises for incident response?

A. Security budget augmentation
B. Process improvements
C. Real-time to remediate
D. Security control selection

Answer: B

NEW QUESTION 514
- (Exam Topic 3)
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 515
- (Exam Topic 3)
In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?

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

Answer: D

NEW QUESTION 516
- (Exam Topic 3)
A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims. Which of the following vendor provided documents is BEST to make your decision:

A. Vendor's client list of reputable organizations currently using their solution
B. Vendor provided attestation of the detailed security controls from a reputable accounting firm
C. Vendor provided reference from an existing reputable client detailing their implementation
D. Vendor provided internal risk assessment and security control documentation

Answer: B

NEW QUESTION 520
- (Exam Topic 3)
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 522
- (Exam Topic 3)
When selecting a security solution with reoccurring maintenance costs after the first year, the CISO should: (choose the BEST answer)

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

Answer: B

NEW QUESTION 523
- (Exam Topic 3)
Which of the following represents the BEST method of ensuring security program alignment to business needs?

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

Answer: B

NEW QUESTION 528
- (Exam Topic 3)
A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?

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

Answer: C

NEW QUESTION 531
- (Exam 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 535
- (Exam Topic 3)
Which of the following is critical in creating a security program aligned with an organization's goals?

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

Answer: B

NEW QUESTION 537
- (Exam 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 539
- (Exam Topic 3)
You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

A. Deploy a SEIM solution and have current staff review incidents first thing in the morning
B. Contract with a managed security provider and have current staff on recall for incident response
C. Configure your syslog to send SMS messages to current staff when target events are triggered
D. Employ an assumption of breach protocol and defend only essential information resources

Answer: B

NEW QUESTION 544
- (Exam Topic 3)
Which business stakeholder is accountable for the integrity of a new information system?

A. CISO
B. Compliance Officer
C. Project manager
D. Board of directors

Answer: A

NEW QUESTION 548
- (Exam 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 551
- (Exam Topic 3)
A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability. What do you do?

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

Answer: C

NEW QUESTION 553
- (Exam Topic 3)
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

A. Alignment with the business
B. Effective use of existing technologies
C. Leveraging existing implementations
D. Proper budget management

Answer: A

NEW QUESTION 555
- (Exam Topic 2)
Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

A. Detective Controls
B. Proactive Controls
C. Preemptive Controls
D. Organizational Controls

Answer: D

NEW QUESTION 560
- (Exam 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 565
- (Exam 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 568
- (Exam Topic 2)
Which of the following are primary concerns for management with regard to assessing internal control objectives?

A. Confidentiality, Availability, Integrity
B. Compliance, Effectiveness, Efficiency
C. Communication, Reliability, Cost
D. Confidentiality, Compliance, Cost

Answer: B

NEW QUESTION 570
- (Exam Topic 2)
Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

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

Answer: D

NEW QUESTION 574
- (Exam Topic 2)
Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

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

D. National Institute of Standards and Technology Special Publication SP 800-26

Answer: A

NEW QUESTION 575
- (Exam Topic 2)
The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

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

Answer: C

NEW QUESTION 578
- (Exam 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 581
- (Exam Topic 2)
As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?

A. Nothing, this falls outside your area of influence.
B. Close and chain the door shut and send a company-wide memo banning the practice.
C. Have a risk assessment performed.
D. Post a guard at the door to maintain physical security

Answer: C

NEW QUESTION 584
- (Exam Topic 2)
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

A. Procedural control
B. Management control
C. Technical control
D. Administrative control

Answer: B

NEW QUESTION 588
- (Exam Topic 2)
The amount of risk an organization is willing to accept in pursuit of its mission is known as

A. Risk mitigation
B. Risk transfer
C. Risk tolerance
D. Risk acceptance

Answer: C

NEW QUESTION 592
- (Exam Topic 2)
Which of the following is the MOST important goal of risk management?

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

Answer: B

NEW QUESTION 595
- (Exam Topic 2)
Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control

requirements, technical issues, and business risks?

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

Answer: A

NEW QUESTION 597
- (Exam 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 602
- (Exam Topic 2)
You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

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

Answer: B

NEW QUESTION 603
- (Exam Topic 2)
Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

A. Meet regulatory compliance requirements
B. Better understand the threats and vulnerabilities affecting the environment
C. Better understand strengths and weaknesses of the program
D. Meet legal requirements

Answer: C

NEW QUESTION 604
- (Exam Topic 2)
Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

A. Perform a vulnerability scan of the network
B. External penetration testing by a qualified third party
C. Internal Firewall ruleset reviews
D. Implement network intrusion prevention systems

Answer: B

NEW QUESTION 607
.....

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