

# 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](https://www.cybok.org/media/downloads/cybok_version_1.0.pdf)

#### NEW QUESTION 2

- (Exam Topic 6)

Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?

- A. Purge
- B. Clear
- C. Mangle
- D. Destroy

**Answer:** B

#### **Explanation:**

Reference:

<https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations>

#### NEW QUESTION 3

- (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 4

- (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 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)

What key technology can mitigate ransomware threats?

- A. Use immutable data storage
- B. Phishing exercises
- C. Application of multiple end point anti-malware solutions
- D. Blocking use of wireless networks

**Answer:** A

#### Explanation:

Reference:

<https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks>

#### NEW QUESTION 8

- (Exam Topic 6)

What does RACI stand for?

- A. Reasonable, Actionable, Controlled, and Implemented
- B. Responsible, Actors, Consult, and Instigate
- C. Responsible, Accountable, Consulted, and Informed
- D. Review, Act, Communicate, and Inform

**Answer:** C

#### Explanation:

Reference: <https://www.google.com/search?q=What+does+RACI+stand+for&oq=What+does+RACI+stand+for&aqs=edge>

#### NEW QUESTION 9

- (Exam Topic 6)

Of the following types of SOC's (Security Operations Centers), which one would be MOST likely used if the CISO has decided to outsource the infrastructure and administration of it?

- A. Virtual
- B. Dedicated
- C. Fusion
- D. Command

**Answer:** A

#### Explanation:

Reference: <https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC>

#### NEW QUESTION 10

- (Exam Topic 6)

Who is responsible for verifying that audit directives are implemented?

- A. IT Management
- B. Internal Audit
- C. IT Security
- D. BOD Audit Committee

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 10

- (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 14

- (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 15

- (Exam Topic 6)

In defining a strategic security plan for an organization, what should a CISO first analyze?

- A. Reach out to a business similar to yours and ask for their plan
- B. Set goals that are difficult to attain to drive more productivity
- C. Review business acquisitions for the past 3 years
- D. Analyze the broader organizational strategic plan

**Answer:** D

**Explanation:**

Reference: <https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/>

#### NEW QUESTION 19

- (Exam 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 20

- (Exam 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 21

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 24

- (Exam 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 26**

- (Exam 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 27**

- (Exam Topic 1)

What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

- A. Determine appetite
- B. Evaluate risk avoidance criteria
- C. Perform a risk assessment
- D. Mitigate risk

**Answer:** D

**NEW QUESTION 28**

- (Exam 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 33**

- (Exam 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 38**

- (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 42**

- (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 44**

- (Exam 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 49

- (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 54

- (Exam Topic 1)

According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

- A. Susceptibility to attack, mitigation response time, and cost
- B. Attack vectors, controls cost, and investigation staffing needs
- C. Vulnerability exploitation, attack recovery, and mean time to repair
- D. Susceptibility to attack, expected duration of attack, and mitigation availability

**Answer:** A

#### NEW QUESTION 59

- (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 63

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 66

- (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 70

- (Exam Topic 1)

Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

- A. Need to comply with breach disclosure laws
- B. Need to transfer the risk associated with hosting PII data
- C. Need to better understand the risk associated with using PII data
- D. Fiduciary responsibility to safeguard credit card information

**Answer:** C

#### NEW QUESTION 72

- (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 77

- (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 78

- (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 79

- (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 81

- (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. A low vulnerability environment
- D. A high risk tolerance environment

**Answer: D**

#### NEW QUESTION 85

- (Exam Topic 1)

The single most important consideration to make when developing your security program, policies, and processes is:

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

**Answer: C**

#### NEW QUESTION 90

- (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 93**

- (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 95**

- (Exam 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 98**

- (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 101**

- (Exam 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 103**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 107**

- (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 110**

- (Exam 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 114**

- (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 118**

- (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 low

**Answer:** C

**NEW QUESTION 122**

- (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 123**

- (Exam 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 126**

- (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 130**

- (Exam Topic 1)

Which of the following should be determined while defining risk management strategies?

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

**Answer:** A

**NEW QUESTION 134**

- (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 135**

- (Exam Topic 1)

Which of the following international standards can be BEST used to define a Risk Management process in an organization?

- A. National Institute for Standards and Technology 800-50 (NIST 800-50)
- B. International Organization for Standardizations – 27005 (ISO-27005)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations – 27004 (ISO-27004)

**Answer:** B

**NEW QUESTION 137**

- (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 140**

- (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 142**

- (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 146**

- (Exam Topic 6)

With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

- A. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
- B. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program
- C. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
- D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

**Answer:** C

**Explanation:**

Reference: [https://nanopdf.com/download/information-security-governance-guidance-for-boards-of\\_pdf](https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf) (9)

#### NEW QUESTION 150

- (Exam 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 154

- (Exam Topic 5)

What is the primary reason for performing a return on investment analysis?

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

**Answer: B**

#### NEW QUESTION 157

- (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 159

- (Exam Topic 5)

SCENARIO: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.

In what phase of the response will the team extract information from the affected systems without altering original data?

- A. Response
- B. Investigation
- C. Recovery
- D. Follow-up

**Answer: B**

#### NEW QUESTION 164

- (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 168

- (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 171

- (Exam Topic 5)

As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

- A. Dual Control
- B. Separation of Duties
- C. Split Knowledge
- D. Least Privilege

**Answer:** A

#### Explanation:

Reference: <https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management>

#### NEW QUESTION 174

- (Exam 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 178

- (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 183

- (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.

Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

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

**Answer:** A

#### NEW QUESTION 186

- (Exam 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 187

- (Exam 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 189**

- (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 192**

- (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 194**

- (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 199**

- (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 203**

- (Exam Topic 5)

Which of the following best describes a portfolio?

- A. The portfolio is used to manage and track individual projects
- B. The portfolio is used to manage incidents and events
- C. A portfolio typically consists of several programs
- D. A portfolio delivers one specific service or program to the business

**Answer:** C

**NEW QUESTION 206**

- (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. Your Corporate Information Security Policy should include which of the following?

- A. Information security theory
- B. Roles and responsibilities
- C. Incident response contacts
- D. Desktop configuration standards

**Answer:** B

**NEW QUESTION 210**

- (Exam Topic 5)

Involvement of senior management is MOST important in the development of:

- A. IT security implementation plans.



- B. Standards and guidelines.
- C. IT security policies.
- D. IT security procedures.

**Answer:** C

**NEW QUESTION 214**

- (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 215**

- (Exam 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 220**

- (Exam 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 224**

- (Exam 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 227**

- (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 230**

- (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 235**

- (Exam Topic 5)

Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

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

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

**Answer: B**

#### NEW QUESTION 240

- (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 243

- (Exam Topic 5)

Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

What action should you take FIRST?

- A. Destroy the repository of stolen data
- B. Contact your local law enforcement agency
- C. Consult with other C-Level executives to develop an action plan
- D. Contract with a credit reporting company for paid monitoring services for affected customers

**Answer: C**

#### NEW QUESTION 247

- (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 250

- (Exam Topic 5)

As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

- A. File Transfer Protocol (FTP)
- B. Virtual Local Area Network (VLAN)
- C. Simple Mail Transfer Protocol
- D. Virtual Private Network (VPN)

**Answer: D**

#### Explanation:

Reference: <https://searchnetworking.techtarget.com/definition/virtual-private-network>

#### NEW QUESTION 253

- (Exam Topic 5)

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



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

**Answer:** D

**NEW QUESTION 255**

- (Exam 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 257**

- (Exam Topic 5)

Which of the following best describes an access control process that confirms the identity of the entity seeking access to a logical or physical area?

- A. Identification
- B. Authorization
- C. Authentication
- D. Accountability

**Answer:** B

**NEW QUESTION 260**

- (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 264**

- (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 265**

- (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 266**

- (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 270**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 274**

- (Exam 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 278**

- (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 279**

- (Exam 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 282**

- (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 283**

- (Exam Topic 3)

When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

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

**Answer:** A

**NEW QUESTION 284**

- (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 286**

- (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 289**

- (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 294**

- (Exam Topic 3)

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

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

**Answer:** B

#### **NEW QUESTION 299**

- (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 302**

- (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 304**

- (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 308**

- (Exam Topic 3)

Which of the following is the BEST indicator of a successful project?

- A. it is completed on time or early as compared to the baseline project plan
- B. it meets most of the specifications as outlined in the approved project definition
- C. it comes in at or below the expenditures planned for in the baseline budget
- D. the deliverables are accepted by the key stakeholders

**Answer:** D

#### NEW QUESTION 312

- (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 317

- (Exam Topic 3)

How often should the SSAE16 report of your vendors be reviewed?

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

**Answer:** C

#### NEW QUESTION 320

- (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 324

- (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 325

- (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 328

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 329**

- (Exam Topic 3)

Which of the following is a major benefit of applying risk levels?

- A. Risk management governance becomes easier since most risks remain low once mitigated
- B. Resources are not wasted on risks that are already managed to an acceptable level
- C. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology
- D. Risk appetite can increase within the organization once the levels are understood

**Answer:** B

**NEW QUESTION 330**

- (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 335**

- (Exam 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 337**

- (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 339**

- (Exam 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 340**

- (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 344**

- (Exam 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 346**

- (Exam Topic 2)

The risk found after a control has been fully implemented is called:

- A. Residual Risk
- B. Total Risk
- C. Post implementation risk
- D. Transferred risk

**Answer:** A

**NEW QUESTION 350**

- (Exam 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 351**

- (Exam Topic 2)

The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

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

**Answer:** D

**NEW QUESTION 353**

- (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 355**

- (Exam Topic 2)

In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

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

**Answer:** C

**NEW QUESTION 357**

- (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 361**

- (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 366**

- (Exam 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 368**

- (Exam 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 371**

- (Exam Topic 2)

You have implemented the new controls. What is the next step?

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

**Answer:** B

#### **NEW QUESTION 374**

- (Exam Topic 2)

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

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

**Answer:** B

#### **NEW QUESTION 376**

- (Exam Topic 2)

Which represents PROPER separation of duties in the corporate environment?

- A. Information Security and Identity Access Management teams perform two distinct functions
- B. Developers and Network teams both have admin rights on servers
- C. Finance has access to Human Resources data
- D. Information Security and Network teams perform two distinct functions

**Answer:** D

#### **NEW QUESTION 378**

- (Exam Topic 2)

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

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

**Answer:** A



**NEW QUESTION 383**

- (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 384**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 389**

- (Exam 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 394**

.....

## 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](#)**