

## Exam Questions 712-50

EC-Council Certified CISO (CCISO)

<https://www.2passeasy.com/dumps/712-50/>



#### NEW QUESTION 1

- (Exam Topic 6)

An auditor is reviewing the security classifications for a group of assets and finds that many of the assets are not correctly classified. What should the auditor's NEXT step be?

- A. Immediately notify the board of directors of the organization as to the finding
- B. Correct the classifications immediately based on the auditor's knowledge of the proper classification
- C. Document the missing classifications
- D. Identify the owner of the asset and induce the owner to apply a proper classification

**Answer:** C

#### NEW QUESTION 2

- (Exam Topic 6)

What is the primary difference between regulations and standards?

- A. Standards will include regulations
- B. Standards that aren't followed are punishable by fines
- C. Regulations are made enforceable by the power provided by laws
- D. Regulations must be reviewed and approved by the business

**Answer:** C

#### NEW QUESTION 3

- (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 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)

A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

- A. Public cloud
- B. Private cloud
- C. Community cloud
- D. Hybrid cloud

**Answer:** D

#### Explanation:

Reference:

<https://www.datacenters.com/services/cloud-services#:~:text=Hybrid%20clouds%20combine%20public%20and>

#### NEW QUESTION 6

- (Exam Topic 6)

When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

- A. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
- B. Contracting rules typically require you to have conversations with two or more groups
- C. Discussing decisions with a very large group of people always provides a better outcome
- D. It helps to avoid regulatory or internal compliance issues

**Answer:** D

**Explanation:**

Reference:

<https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf>

**NEW QUESTION 7**

- (Exam Topic 6)

A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP). In developing the business impact assessment (BIA), which of the following MOST closely relate to the data backup and restoral?

- A. Recovery Point Objective (RPO)
- B. Mean Time to Delivery (MTD)
- C. Recovery Time Objective (RTO)
- D. Maximum Tolerable Downtime (MTD)

**Answer:** C

**Explanation:**

Reference:

<https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#:~:text=The%2>

**NEW QUESTION 8**

- (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 9**

- (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 10**

- (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)

An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.

What is the MOST likely reason why the sensitive data was posted?

- A. The DLP Solution was not integrated with mobile device anti-malware
- B. Data classification was not properly performed on the assets
- C. The sensitive data was not encrypted while at rest
- D. A risk assessment was not performed after purchasing the DLP solution

**Answer:** D

#### NEW QUESTION 13

- (Exam Topic 6)

A bastion host should be placed:

- A. Inside the DMZ
- B. In-line with the data center firewall
- C. Beyond the outer perimeter firewall
- D. As the gatekeeper to the organization's honeynet

**Answer:** C

#### Explanation:

Reference: <https://www.skillset.com/questions/a-bastion-host-is-which-of-the-following>

#### NEW QUESTION 15

- (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 18

- (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 22

- (Exam Topic 2)

How often should an environment be monitored for cyber threats, risks, and exposures?

- A. Weekly
- B. Monthly
- C. Quarterly
- D. Daily

**Answer:** D

#### NEW QUESTION 27

- (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 32

- (Exam Topic 2)

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

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

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

**Answer:** A

#### NEW QUESTION 36

- (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 39

- (Exam Topic 2)

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

- A. Daily
- B. Hourly
- C. Weekly
- D. Monthly

**Answer:** A

#### NEW QUESTION 42

- (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 46

- (Exam Topic 2)

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

- A. A substantive test of program library controls
- B. A compliance test of program library controls
- C. A compliance test of the program compiler controls
- D. A substantive test of the program compiler controls

**Answer:** B

#### NEW QUESTION 51

- (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 52

- (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 54

- (Exam Topic 1)

When choosing a risk mitigation method what is the MOST important factor?

- A. Approval from the board of directors
- B. Cost of the mitigation is less than the risk
- C. Metrics of mitigation method success
- D. Mitigation method complies with PCI regulations

**Answer:** B

#### NEW QUESTION 56

- (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 59

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 62

- (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 65

- (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 67

- (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 68

- (Exam Topic 1)

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

- A. Multiple certifications, strong technical capabilities and lengthy resume
- B. Industry certifications, technical knowledge and program management skills
- C. College degree, audit capabilities and complex project management
- D. Multiple references, strong background check and industry certifications



Answer: B

#### NEW QUESTION 69

- (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 70

- (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 71

- (Exam Topic 1)

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

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

Answer: B

#### NEW QUESTION 74

- (Exam Topic 1)

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

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

Answer: B

#### NEW QUESTION 76

- (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 78

- (Exam Topic 1)

Who is responsible for securing networks during a security incident?

- A. Chief Information Security Officer (CISO)
- B. Security Operations Center (SOC)
- C. Disaster Recovery (DR) manager
- D. Incident Response Team (IRT)

Answer: D

#### NEW QUESTION 80

- (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 84

- (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 87

- (Exam Topic 1)

Which of the following intellectual Property components is focused on maintaining brand recognition?

- A. Trademark
- B. Patent
- C. Research Logs
- D. Copyright

**Answer:** A

#### NEW QUESTION 91

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 95

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 100

- (Exam Topic 1)

Risk is defined as:

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

**Answer:** A

#### NEW QUESTION 101

- (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 105

- (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 110

- (Exam Topic 1)

The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

- A. Due Protection
- B. Due Care
- C. Due Compromise
- D. Due process

**Answer:** B

#### NEW QUESTION 111

- (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 114

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 118

- (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 119

- (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 123

- (Exam Topic 1)

Why is it vitally important that senior management endorse a security policy?

- A. So that they will accept ownership for security within the organization.
- B. So that employees will follow the policy directives.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they can be held legally accountable.

**Answer:** A

#### NEW QUESTION 128

- (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 130

- (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 135

- (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 137

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 142

- (Exam Topic 1)

Which of the following provides an audit framework?

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

**Answer:** A

#### NEW QUESTION 145

- (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 149

- (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 154

- (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 158

- (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 163

- (Exam Topic 6)

Which of the following statements below regarding Key Performance indicators (KPIs) are true?

- A. Development of KPI's are most useful when done independently
- B. They are a strictly quantitative measure of success
- C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
- D. They are a strictly qualitative measure of success

**Answer:** A

#### Explanation:

Reference: <https://kpi.org/KPI-Basics/KPI-Development>

#### NEW QUESTION 168

- (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 171

- (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 174

- (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 177**

- (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 181**

- (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 adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

- A. Annually
- B. Semi-annually
- C. Quarterly
- D. Never

**Answer: D**

**NEW QUESTION 185**

- (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 188**

- (Exam Topic 5)

A digital signature addresses which of the following concerns?

- A. Message alteration
- B. Message copying
- C. Message theft
- D. Unauthorized reading

**Answer: A**

**Explanation:**

Reference: <https://www.entrust.com/resources/certificate-solutions/learn/digital-signatures>

**NEW QUESTION 192**

- (Exam Topic 5)

Which of the following information would MOST likely be reported at the board-level within an organization?

- A. System scanning trends and results as they pertain to insider and external threat sources
- B. The capabilities of a security program in terms of staffing support
- C. Significant risks and security incidents that have been discovered since the last assembly of the membership
- D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

**Answer: C**

**NEW QUESTION 196**

- (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 201

- (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 206

- (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 210

- (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 211

- (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 214

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

**Answer:** C

#### NEW QUESTION 216

- (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 219



- (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 220

- (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 223

- (Exam Topic 5)

The new CISO was informed of all the Information Security projects that the organization has in progress. Two projects are over a year behind schedule and over budget. Using best business practices for project management you determine that the project correctly aligns with the company goals.

Which of the following needs to be performed NEXT?

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

**Answer:** A

#### NEW QUESTION 225

- (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 227

- (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 229

- (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 234



- (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.

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

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

**Answer: D**

#### NEW QUESTION 235

- (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 239

- (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.

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

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

**Answer: B**

#### NEW QUESTION 242

- (Exam Topic 5)

At what level of governance are individual projects monitored and managed?

- A. Program
- B. Milestone
- C. Enterprise
- D. Portfolio

**Answer: D**

#### NEW QUESTION 243

- (Exam Topic 5)

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. Effective use of existing technologies
- B. Create a comprehensive security awareness program and provide success metrics to business units
- C. Proper budget management
- D. Leveraging existing implementations

**Answer: B**

#### NEW QUESTION 247

- (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/](http://www.umsl.edu/~sauterv/analysis/6840_f03_papers/gurlen/)

**NEW QUESTION 248**

- (Exam Topic 5)

If the result of an NPV is positive, then the project should be selected. The net present value shows the present value of the project, based on the decisions taken for its selection. What is the net present value equal to?

- A. Net profit – per capita income
- B. Total investment – Discounted cash
- C. Average profit – Annual investment
- D. Initial investment – Future value

**Answer:** C

**NEW QUESTION 249**

- (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 252**

- (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 255**

- (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 256**

- (Exam Topic 5)

Where does bottom-up financial planning primarily gain information for creating budgets?

- A. By adding all capital and operational costs from the prior budgetary cycle, and determining potential financial shortages
- B. By reviewing last year's program-level costs and adding a percentage of expected additional portfolio costs
- C. By adding the cost of all known individual tasks and projects that are planned for the next budgetary cycle
- D. By adding all planned operational expenses per quarter then summarizing them in a budget request

**Answer:** D

**NEW QUESTION 257**

- (Exam Topic 5)

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

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

**Answer:** B

**NEW QUESTION 262**

- (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 266

- (Exam Topic 5)

If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the BEST control to safeguard data integrity?

- A. Backup to tape
- B. Maintain separate VM backups
- C. Backup to a remote location
- D. Increase VM replication frequency

**Answer: B**

#### Explanation:

Reference:

<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/is-audit-basics-backup-andrecovery>

#### NEW QUESTION 267

- (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 268

- (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 272

- (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 277

- (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 280

- (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 282

- (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 284

- (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 289

- (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 293

- (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 297

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 298

- (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 303

- (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 305

- (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 308

- (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 311

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 315

- (Exam Topic 4)

Which of the following is a countermeasure to prevent unauthorized database access from web applications?

- A. Session encryption
- B. Removing all stored procedures
- C. Input sanitization
- D. Library control

**Answer:** C

#### NEW QUESTION 317

- (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 319**

- (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 321**

- (Exam Topic 4)

Which of the following backup sites takes the longest recovery time?

- A. Cold site
- B. Hot site
- C. Warm site
- D. Mobile backup site

**Answer:** A

**NEW QUESTION 322**

- (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 324**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 326**

- (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 330**

- (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 332**

- (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 336

- (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 339

- (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 340

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 342

- (Exam Topic 3)

Your company has a "no right to privacy" notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee's email account. What should you do? (choose the BEST answer):

- A. Grant her access, the employee has been adequately warned through the AUP.
- B. Assist her with the request, but only after her supervisor signs off on the action.
- C. Reset the employee's password and give it to the supervisor.
- D. Deny the request citing national privacy laws.

**Answer:** B

#### NEW QUESTION 347

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 350

- (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 351

- (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 354

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 359

- (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 363

- (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 364

- (Exam Topic 3)

An example of professional unethical behavior is:

- A. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation
- B. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
- C. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
- D. Storing client lists and other sensitive corporate internal documents on a removable thumb drive

**Answer:** C

#### NEW QUESTION 369

- (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 371

- (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 372

- (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 377

- (Exam Topic 3)

When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization. Which example below is the MOST creative way to maintain a strong security posture during these difficult times?

- A. Download open source security tools and deploy them on your production network
- B. Download trial versions of commercially available security tools and deploy on your production network
- C. Download open source security tools from a trusted site, test, and then deploy on production network
- D. Download security tools from a trusted source and deploy to production network

**Answer:** C

#### NEW QUESTION 382

- (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 387

- (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 392

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 396

- (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 401

- (Exam Topic 3)

Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

- A. System testing
- B. Risk assessment
- C. Incident response
- D. Planning

**Answer:** A

#### NEW QUESTION 406

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 408

- (Exam Topic 3)

When should IT security project management be outsourced?

- A. When organizational resources are limited
- B. When the benefits of outsourcing outweigh the inherent risks of outsourcing
- C. On new, enterprise-wide security initiatives
- D. On projects not forecasted in the yearly budget

**Answer:** B

#### NEW QUESTION 410

- (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 411

- (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 416

- (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 419

- (Exam Topic 2)

Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

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

**Answer:** C

**NEW QUESTION 424**

- (Exam Topic 2)

Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

- A. Security Administrators
- B. Internal/External Audit
- C. Risk Management
- D. Security Operations

**Answer:** B

**NEW QUESTION 429**

- (Exam Topic 2)

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

- A. Plan-Check-Do-Act
- B. Plan-Do-Check-Act
- C. Plan-Select-Implement-Evaluate
- D. SCORE (Security Consensus Operational Readiness Evaluation)

**Answer:** B

**NEW QUESTION 430**

- (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 435**

- (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 440**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 441**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 442**

- (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 443**

- (Exam Topic 2)

Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

- A. Single Loss Expectancy (SLE)
- B. Exposure Factor (EF)
- C. Annualized Rate of Occurrence (ARO)
- D. Temporal Probability (TP)

**Answer:** C

**NEW QUESTION 446**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 712-50 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 712-50 Product From:

<https://www.2passeasy.com/dumps/712-50/>

## Money Back Guarantee

### 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