

# EC-Council

## Exam Questions 712-50

EC-Council Certified CISO (CCISO)



#### NEW QUESTION 1

- (Exam Topic 6)

An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO).

The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?

- A. ISO 22318 Supply Chain Continuity
- B. ISO 27031 BCM Readiness
- C. ISO 22301 BCM Requirements
- D. ISO 22317 BIA

**Answer:** C

#### Explanation:

Reference: <https://www.smartsheet.com/content/iso-22301-business-continuity-guide>

#### NEW QUESTION 2

- (Exam Topic 6)

What is the MOST critical output of the incident response process?

- A. A complete document of all involved team members and the support they provided
- B. Recovery of all data from affected systems
- C. Lessons learned from the incident, so they can be incorporated into the incident response processes
- D. Clearly defined documents detailing standard evidence collection and preservation processes

**Answer:** C

#### Explanation:

Reference: <https://www.eccouncil.org/incident-response-plan-phases/>

#### NEW QUESTION 3

- (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 4

- (Exam Topic 6)

During a cyber incident, which non-security personnel might be needed to assist the security team?

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

**Answer:** A

#### NEW QUESTION 5

- (Exam Topic 6)

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 6

- (Exam Topic 6)

A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

- A. Inability to export the private certificate/key
- B. It can double as physical identification at the DMV
- C. It has the user's photograph to help ID them
- D. It can be used as a secure flash drive

**Answer:** C

**Explanation:**

Reference: <https://www.securew2.com/blog/piv-personal-identity-verification>

#### NEW QUESTION 7

- (Exam Topic 6)

What organizational structure combines the functional and project structures to create a hybrid of the two?

- A. Traditional
- B. Composite
- C. Project
- D. Matrix

**Answer:** D

**Explanation:**

Reference: <https://www.knowledgehut.com/tutorials/project-management/organization-structures>

#### NEW QUESTION 8

- (Exam Topic 6)

Which of the following are the triple constraints of project management?

- A. Time, quality, and scope
- B. Cost, quality, and time
- C. Scope, time, and cost
- D. Quality, scope, and cost

**Answer:** C

**Explanation:**

Reference:

<https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%>

#### NEW QUESTION 9

- (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 10

- (Exam Topic 6)

When performing a forensic investigation, what are the two MOST common data sources for obtaining evidence from a computer and mobile devices?

- A. RAM and unallocated space
- B. Unallocated space and RAM
- C. Slack space and browser cache
- D. Persistent and volatile data

**Answer:** D

**Explanation:**

Reference: <https://study.com/academy/lesson/data-storage-formats-digital-forensics-devices-types.html>

#### NEW QUESTION 10

- (Exam Topic 6)

Which of the following is the MOST effective method to counter phishing attacks?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 12**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 14**

- (Exam Topic 2)

When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

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

**Answer:** C

**NEW QUESTION 19**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 24**

- (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 25**

- (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 26**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 27**

- (Exam Topic 1)

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

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

**Answer:** A

#### **NEW QUESTION 32**

- (Exam Topic 1)

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

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

**Answer:** B

#### **NEW QUESTION 37**

- (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 40**

- (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 44**

- (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 49**

- (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 50**

- (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 55

- (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 58

- (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 Information Security Management program MUST protect:

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

**Answer: B**

#### NEW QUESTION 65

- (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 is the MOST important for a CISO to understand when identifying threats?

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

**Answer: A**

#### NEW QUESTION 74

- (Exam Topic 1)

What is a difference from the list below between quantitative and qualitative Risk Assessment?

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

**Answer: A**

#### NEW QUESTION 78

- (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 83**

- (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 85**

- (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 87**

- (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 91**

- (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 95**

- (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 100**

- (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 105**

- (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 110**

- (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 114**

- (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 117**

- (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 122**

- (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 124**

- (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 129**

- (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 133**

- (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 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)

A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

- A. Providing a risk program governance structure
- B. Ensuring developers include risk control comments in code
- C. Creating risk assessment templates based on specific threats
- D. Allowing for the acceptance of risk for regulatory compliance requirements

**Answer:** A

#### NEW QUESTION 140

- (Exam Topic 1)

Payment Card Industry (PCI) compliance requirements are based on what criteria?

- A. The types of cardholder data retained
- B. The duration card holder data is retained
- C. The size of the organization processing credit card data
- D. The number of transactions performed per year by an organization

**Answer:** D

#### NEW QUESTION 144

- (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 146

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 150

- (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 152

- (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 154

- (Exam Topic 1)

In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

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

**Answer:** B

#### NEW QUESTION 158

- (Exam Topic 6)

You have been promoted to the CISO of a big-box retail store chain reporting to the Chief Information Officer (CIO). The CIO's first mandate to you is to develop a cybersecurity compliance framework that will meet all the store's compliance requirements.

Which of the following compliance standard is the MOST important to the organization?

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

**Answer:** D

#### Explanation:

Reference:

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

#### NEW QUESTION 162

- (Exam Topic 6)

Many successful cyber-attacks currently include:

- A. Phishing Attacks
- B. Misconfigurations
- C. Social engineering
- D. All of these

**Answer:** C

#### Explanation:

Reference: <https://www.eccouncil.org/what-is-social-engineering/>

#### NEW QUESTION 165

- (Exam Topic 6)

As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity.

The performance quality audit activity is done in what project management process group?

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

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 169

- (Exam Topic 6)

A CISO must conduct risk assessments using a method where the Chief Financial Officer (CFO) receives impact data in financial terms to use as input to select the proper level of coverage in a new cybersecurity insurance policy.

What is the MOST effective method of risk analysis to provide the CFO with the information required?

- A. Conduct a quantitative risk assessment

- B. Conduct a hybrid risk assessment
- C. Conduct a subjective risk assessment
- D. Conduct a qualitative risk assessment

**Answer:** D

#### NEW QUESTION 173

- (Exam Topic 5)

Which of the following best describes the sensors designed to project and detect a light beam across an area?

- A. Smoke
- B. Thermal
- C. Air-aspirating
- D. Photo electric

**Answer:** D

#### Explanation:

Reference: [https://en.wikipedia.org/wiki/Photoelectric\\_sensor](https://en.wikipedia.org/wiki/Photoelectric_sensor)

#### NEW QUESTION 175

- (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)

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 180

- (Exam Topic 5)

What are the three stages of an identity and access management system?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 185

- (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 190

- (Exam Topic 5)

What are the three hierarchically related aspects of strategic planning and in which order should they be done?

- A. 1) Information technology strategic planning, 2) Enterprise strategic planning, 3) Cybersecurity or information security strategic planning
- B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3) Information technology strategic planning

- C. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning  
D. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3) Information technology strategic planning

**Answer:** D

#### NEW QUESTION 191

- (Exam Topic 5)

Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

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

**Answer:** A

#### NEW QUESTION 194

- (Exam Topic 5)

Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.

Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

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

**Answer:** C

#### NEW QUESTION 195

- (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 199

- (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 204

- (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 209

- (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 211**

- (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 213**

- (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 218**

- (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 220**

- (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 222**

- (Exam Topic 5)

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

How can you reduce the administrative burden of distributing symmetric keys for your employer?

- A. Use asymmetric encryption for the automated distribution of the symmetric key
- B. Use a self-generated key on both ends to eliminate the need for distribution
- C. Use certificate authority to distribute private keys
- D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

**Answer:** A

**NEW QUESTION 223**

- (Exam Topic 5)

What are the primary reasons for the development of a business case for a security project?

- A. To estimate risk and negate liability to the company
- B. To understand the attack vectors and attack sources
- C. To communicate risk and forecast resource needs
- D. To forecast usage and cost per software licensing

**Answer:** C



#### NEW QUESTION 225

- (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.

During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical aspect of the team's activities?

- A. Regular communication of incident status to executives
- B. Eradication of malware and system restoration
- C. Determination of the attack source
- D. Preservation of information

**Answer: D**

#### NEW QUESTION 229

- (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 230

- (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 234

- (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 235

- (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 236

- (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 241

- (Exam Topic 5)

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

Symmetric encryption in general is preferable to asymmetric encryption when:

- A. The number of unique communication links is large
- B. The volume of data being transmitted is small
- C. The speed of the encryption / deciphering process is essential
- D. The distance to the end node is farthest away

**Answer: C**

#### NEW QUESTION 246

- (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 247

- (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.”

Which group of people should be consulted when developing your security program?

- A. Peers
- B. End Users
- C. Executive Management
- D. All of the above

**Answer: D**

#### NEW QUESTION 251

- (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 254

- (Exam Topic 5)

When dealing with risk, the information security practitioner may choose to:

- A. assign
- B. transfer
- C. acknowledge
- D. defer

**Answer: C**

#### NEW QUESTION 256

- (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 261



- (Exam Topic 5)

Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.

You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

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

**Answer:** A

#### NEW QUESTION 262

- (Exam Topic 5)

The total cost of security controls should:

- A. Be equal to the value of the information resource being protected
- B. Be greater than the value of the information resource being protected
- C. Be less than the value of the information resource being protected
- D. Should not matter, as long as the information resource is protected

**Answer:** C

#### NEW QUESTION 266

- (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 269

- (Exam Topic 5)

Which of the following is the MOST logical method of deploying security controls within an organization?

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

**Answer:** B

#### NEW QUESTION 274

- (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 275

- (Exam Topic 5)

What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

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

**Answer:** B

#### Explanation:

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

**NEW QUESTION 276**

- (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 280**

- (Exam Topic 5)

Which technology can provide a computing environment without requiring a dedicated hardware backend?

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

**Answer:** B

**NEW QUESTION 284**

- (Exam Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. The organization wants a more permanent solution to the threat to user credential compromise through phishing. What technical solution would BEST address this issue?

- A. Professional user education on phishing conducted by a reputable vendor
- B. Multi-factor authentication employing hard tokens
- C. Forcing password changes every 90 days
- D. Decreasing the number of employees with administrator privileges

**Answer:** B

**NEW QUESTION 288**

- (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 292**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 297**

- (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 302**

- (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 307**

- (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 310**

- (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 311**

- (Exam Topic 4)

Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?

- A. Comprehensive Log-Files from all servers and network devices affected during the attack
- B. Fully trained network forensic experts to analyze all data right after the attack
- C. Uninterrupted Chain of Custody
- D. Expert forensics witness

**Answer:** C

**NEW QUESTION 314**

- (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 316**

- (Exam Topic 4)

Which wireless encryption technology makes use of temporal keys?

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

**Answer:** B

**NEW QUESTION 319**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 323**

- (Exam Topic 3)

You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

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

**Answer: B**

#### **NEW QUESTION 325**

- (Exam Topic 3)

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

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

**Answer: A**

#### **NEW QUESTION 328**

- (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)

Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

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

**Answer: C**

#### **NEW QUESTION 334**

- (Exam Topic 3)

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

- A. Cost benefit
- B. Risk appetite
- C. Business continuity
- D. Likelihood of impact

**Answer: B**

#### **NEW QUESTION 336**

- (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)

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

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

**Answer: C**

**NEW QUESTION 345**

- (Exam Topic 3)

Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

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

**Answer: C**

**NEW QUESTION 347**

- (Exam Topic 3)

Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

- A. Risk Management
- B. Risk Assessment
- C. System Testing
- D. Vulnerability Assessment

**Answer: B**

**NEW QUESTION 351**

- (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 355**

- (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 356**

- (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 357**

- (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 359**

- (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 361**

- (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 365**

- (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 368**

- (Exam Topic 3)

The ultimate goal of an IT security projects is:

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

**Answer: C**

**NEW QUESTION 369**

- (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 371**

- (Exam Topic 3)

When managing the critical path of an IT security project, which of the following is MOST important?

- A. Knowing who all the stakeholders are.
- B. Knowing the people on the data center team.
- C. Knowing the threats to the organization.
- D. Knowing the milestones and timelines of deliverables.

**Answer: D**

**NEW QUESTION 373**

- (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 376**

- (Exam Topic 2)

An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application. What should be the NEXT step?



- A. Determine the annual loss expectancy (ALE)
- B. Create a crisis management plan
- C. Create technology recovery plans
- D. Build a secondary hot site

**Answer: C**

**NEW QUESTION 378**

- (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 380**

- (Exam Topic 2)

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

- A. Senior Executives
- B. Office of the Auditor
- C. Office of the General Counsel
- D. All employees and users

**Answer: A**

**NEW QUESTION 383**

- (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 385**

- (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 390**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 392**

- (Exam Topic 2)

As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

- A. Executive summary
- B. Penetration test agreement
- C. Names and phone numbers of those who conducted the audit
- D. Business charter

**Answer: A**



**NEW QUESTION 396**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 401**

- (Exam Topic 2)

The amount of risk an organization is willing to accept in pursuit of its mission is known as

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

**Answer: C**

**NEW QUESTION 405**

- (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 410**

- (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 413**

- (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 417**

- (Exam Topic 2)

Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

- A. ISO 27001
- B. ISO 27002
- C. ISO 27004
- D. ISO 27005

**Answer: D**

**NEW QUESTION 422**

- (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 426**

- (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 427**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 429**

.....

## 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](#)**