ECCouncil

Exam 712-50

EC-Council Certified CISO (CCISO)

Version: 6.0

[Total Questions: 343]

Topic break down

Topic	No. of Questions
Topic 1: Governance (Policy, Legal & Compliance)	97
Topic 2: IS Management Controls and Auditing Management	75
Topic 3: Management – Projects and Operations (Projects, Technology & Operations)	68
Topic 4: Information Security Core Competencies	30
Topic 5: Strategic Planning & Finance.	73

Topic 1, Governance (Policy, Legal & Compliance)

Question No : 1 - (Topic 1)

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

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

Answer: B

Question No : 2 - (Topic 1)

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

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

Answer: C

Question No : 3 - (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

Question No : 4 - (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

Question No : 5 - (Topic 1)

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer: A

Question No : 6 - (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

Question No : 7 - (Topic 1)

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

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

Answer: C

Question No : 8 - (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

Question No : 9 - (Topic 1)

A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?

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

Answer: C

Question No : 10 - (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

Question No : 11 - (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

Question No : 12 - (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

Question No : 13 - (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

Question No : 14 - (Topic 1)

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

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

Answer: C

Question No : 15 - (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

Question No : 16 - (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

Question No : 17 - (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

Question No : 18 - (Topic 1)

You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

A. Controlled mitigation effort
B. Risk impact comparison
C. Relative likelihood of event
D. Comparative threat analysis

Answer: C

Question No : 19 - (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

Question No : 20 - (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

Question No : 21 - (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

Question No : 22 - (Topic 1)

When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

A. In promiscuous mode and only detect malicious traffic.

B. In-line and turn on blocking mode to stop malicious traffic.

C. In promiscuous mode and block malicious traffic.

D. In-line and turn on alert mode to stop malicious traffic.

Answer: B

Question No : 23 - (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

Question No : 24 - (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

Question No : 25 - (Topic 1)

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

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