# EC-Council 712-50 Exam

**Volume: 343 Questions**

Question: 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

Question: 2
Developing effective security controls is a balance between:

A. Risk Management and Operations

B. Corporate Culture and Job Expectations

C. Operations and Regulations

D. Technology and Vendor Management

Answer: A

Question: 3
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

Question: 4
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

Question: 5
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: 6
The alerting, monitoring and life-cycle management of security related events is typically handled by the

A. security threat and vulnerability management process

B. risk assessment process

C. risk management process

D. governance, risk, and compliance tools

Answer: A

Question: 7
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

Question: 8
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

Question: 9
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

Question: 10
Which of the following is a critical operational component of an Incident Response Program (IRP)?

A. Weekly program budget reviews to ensure the percentage of program funding remains constant.

B. Annual review of program charters, policies, procedures and organizational agreements.

C. Daily monitoring of vulnerability advisories relating to your organization's deployed technologies.

D. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization

Answer: C

Question: 11
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

Question: 12
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

A. Audit and Legal

B. Budget and Compliance

C. Human Resources and Budget

D. Legal and Human Resources

Answer: A

Question: 13
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: 14
Which of the following is a benefit of information security governance?

A. Questioning the trust in vendor relationships.

B. Increasing the risk of decisions based on incomplete management information.

C. Direct involvement of senior management in developing control processes

D. Reduction of the potential for civil and legal liability

Answer: D

Question: 15
The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope

B. Getting authority to operate the system from executive management

C. Changing the default passwords

D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

Question: 16
Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

A. Need to comply with breach disclosure laws

B. Need to transfer the risk associated with hosting PII data

C. Need to better understand the risk associated with using PII data

D. Fiduciary responsibility to safeguard credit card information

Answer: C

Question: 17
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: 18
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: 19
Which of the following is the MOST important benefit of an effective security governance process?

A. Reduction of liability and overall risk to the organization

B. Better vendor management

C. Reduction of security breaches

D. Senior management participation in the incident response process

Answer: A

Question: 20
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

Question: 21
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

Question: 22
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

Question: 23
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: 24

Which of the following has the GREATEST impact on the implementation of an information security governance model?

A. Organizational budget

B. Distance between physical locations

C. Number of employees

D. Complexity of organizational structure

Answer: D

Question: 25
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: 26
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

Question: 27
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

Question: 28
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

Question: 29
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