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)

After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

A. Risk Tolerance
B. Qualitative risk analysis
C. Risk Appetite
D. Quantitative risk analysis

Answer: D

Question No : 2 - (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 : 3 - (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

Question No : 4 - (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

Question No : 5 - (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

Question No : 6 - (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 : 7 - (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

Question No : 8 - (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 : 9 - (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

Question No : 10 - (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

Question No : 11 - (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 : 12 - (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

Answer: B

Question No : 13 - (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

Question No : 14 - (Topic 1)

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

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

Answer: D

Question No : 15 - (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 : 16 - (Topic 1)

The FIRST step in establishing a security governance program is to?

A. Conduct a risk assessment.
B. Obtain senior level sponsorship.
C. Conduct a workshop for all end users.
D. Prepare a security budget.

Answer: B

Question No : 17 - (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

Question No : 18 - (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 : 19 - (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

Question No : 20 - (Topic 1)

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization’s need?

A. International Organization for Standardizations – 22301 (ISO-22301)
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27005 (ISO-27005)

Answer: A

Question No : 21 - (Topic 1)

Risk appetite directly affects what part of a vulnerability management program?

A. Staff
B. Scope
C. Schedule
D. Scan tools

Answer: B

Question No : 22 - (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

Question No : 23 - (Topic 1)

An organization information security policy serves to

A. establish budgetary input in order to meet compliance requirements
B. establish acceptable systems and user behavior
C. define security configurations for systems
D. define relationships with external law enforcement agencies

Answer: B

Question No : 24 - (Topic 1)

When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

A. Escalation
B. Recovery
C. Eradication
D. Containment

Answer: D

Question No : 25 - (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

Question No : 26 - (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 : 27 - (Topic 1)

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 No : 28 - (Topic 1)

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

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

Answer: B

Question No : 29 - (Topic 1)

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

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

Answer: C

Question No : 30 - (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 : 31 - (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

Question No : 32 - (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 lo

Answer: C

Question No : 33 - (Topic 1)

A method to transfer risk is to:

A. Implement redundancy
B. move operations to another region
C. purchase breach insurance
D. Alignment with business operations

Answer: C

Question No : 34 - (Topic 1)

Which of the following is MOST important when dealing with an Information Security Steering committee:

A. Include a mix of members from different departments and staff levels.
B. Ensure that security policies and procedures have been vetted and approved.
C. Review all past audit and compliance reports.
D. Be briefed about new trends and products at each meeting by a vendor.

Answer: C

Question No : 35 - (Topic 1)

Which of the following is MOST likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

Answer: C

Question No : 36 - (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 : 37 - (Topic 1)

Within an organization’s vulnerability management program, who has the responsibility to implement remediation actions?

A. Security officer
B. Data owner
C. Vulnerability engineer
D. System administrator

Answer: D

Question No : 38 - (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 : 39 - (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

Question No : 40 - (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 : 41 - (Topic 1)

If your organization operates under a model of "assumption of breach", you should:

A. Protect all information resource assets equally
B. Establish active firewall monitoring protocols
C. Purchase insurance for your compliance liability
D. Focus your security efforts on high value assets

Answer: C

Question No : 42 - (Topic 1)

What is the relationship between information protection and regulatory compliance?

A. That all information in an organization must be protected equally.
B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
C. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.
D. There is no relationship between the two.

Answer: C

Question No : 43 - (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 : 44 - (Topic 1)

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

A. Audit and Legal
B. Budget and Compliance
C. Human Resources and Budget
D. Legal and Human Resources

Answer: A

Question No : 45 - (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

Question No : 46 - (Topic 1)

The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.
B. Establishing strategic alignment with bunsiness continuity requirements
C. Establishing incident response programs.
D. Identifying and implementing the best security solutions.

Answer: A

Question No : 47 - (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 : 48 - (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 : 49 - (Topic 1)

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

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

Answer: A

Question No : 50 - (Topic 1)

You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

A. Chief Information Security Officer
B. Chief Executive Officer
C. Chief Information Officer
D. Chief Legal Counsel

Answer: B

Question No : 51 - (Topic 1)

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 No : 52 - (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

Question No : 53 - (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

Question No : 54 - (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

Question No : 55 - (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

Question No : 56 - (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 : 57 - (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

Question No : 58 - (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 : 59 - (Topic 1)

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

A. information security metrics.
B. knowledge required to analyze each issue.

C. baseline against which metrics are evaluated.
D. linkage to business area objectives.

Answer: D

Question No : 60 - (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 : 61 - (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

Question No : 62 - (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 : 63 - (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. I low vulnerability environment
D. A high risk tolerance environment

Answer: D

Question No : 64 - (Topic 1)

What is the definition of Risk in Information Security?

A. Risk = Probability x Impact
B. Risk = Threat x Probability
C. Risk = Financial Impact x Probability
D. Risk = Impact x Threat

Answer: A

Question No : 65 - (Topic 1)

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 No : 66 - (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

Question No : 67 - (Topic 1)

A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

A. Compliance to the Payment Card Industry (PCI) regulations.
B. Alignment with financial reporting regulations for each country where they operate.
C. Alignment with International Organization for Standardization (ISO) standards.
D. Compliance with patient data protection regulations for each country where they operate.

Answer: D

Question No : 68 - (Topic 1)

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

A. Weekly program budget reviews to ensure the percentage of program funding remains constant.
B. Annual review of program charters, policies, procedures and organizational agreements.
C. Daily monitoring of vulnerability advisories relating to your organization’s deployed technologies.
D. Monthly program tests to ensure resource allocation is sufficient for supporting the

needs of the organization

Answer: C

Question No : 69 - (Topic 1)

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 No : 70 - (Topic 1)

Regulatory requirements typically force organizations to implement

A. Mandatory controls
B. Discretionary controls
C. Optional controls
D. Financial controls

Answer: A

Question No : 71 - (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 : 72 - (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

Question No : 73 - (Topic 1)

What is the first thing that needs to be completed in order to create a security program for your organization?

A. Risk assessment
B. Security program budget
C. Business continuity plan
D. Compliance and regulatory analysis

Answer: A

Question No : 74 - (Topic 1)

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 No : 75 - (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 : 76 - (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 : 77 - (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

Question No : 78 - (Topic 1)

Credit card information, medical data, and government records are all examples of:

A. Confidential/Protected Information
B. Bodily Information
C. Territorial Information
D. Communications Information

Answer: A

Question No : 79 - (Topic 1)

Who is responsible for securing networks during a security incident?

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

Answer: D

Question No : 80 - (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 : 81 - (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

Question No : 82 - (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

Question No : 83 - (Topic 1)

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

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

Answer: C

Question No : 84 - (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

Question No : 85 - (Topic 1)

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

A. Contacting the Internet Service Provider for an IP scope
B. Getting authority to operate the system from executive management
C. Changing the default passwords
D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

Question No : 86 - (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

Question No : 87 - (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

Question No : 88 - (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

Question No : 89 - (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

Question No : 90 - (Topic 1)

The exposure factor of a threat to your organization is defined by?

A. Asset value times exposure factor
B. Annual rate of occurrence
C. Annual loss expectancy minus current cost of controls

D. Percentage of loss experienced due to a realized threat event

Answer: D

Question No : 91 - (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

Question No : 92 - (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 : 93 - (Topic 1)

What role should the CISO play in properly scoping a PCI environment?

A. Validate the business units' suggestions as to what should be included in the scoping process
B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment
C. Ensure internal scope validation is completed and that an assessment has been done to

discover all credit card data
D. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope

Answer: C

Question No : 94 - (Topic 1)

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

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

Answer: A

Question No : 95 - (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

Question No : 96 - (Topic 1)

Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

A. Reduction of budget

B. Decreased security awareness
C. Improper use of information resources
D. Fines for regulatory non-compliance

Answer: D

Question No : 97 - (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

Topic 2, IS Management Controls and Auditing Management

Question No : 98 - (Topic 2)

Dataflow diagrams are used by IT auditors to:

A. Order data hierarchically.
B. Highlight high-level data definitions.
C. Graphically summarize data paths and storage processes.
D. Portray step-by-step details of data generation.

Answer: C

Question No : 99 - (Topic 2)

Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

A. It allows executives to more effectively monitor IT implementation costs
B. Implementation of it eases an organization's auditing and compliance burden
C. Information Security (IS) procedures often require augmentation with other standards
D. It provides for a consistent and repeatable staffing model for technology organizations

Answer: B

Question No : 100 - (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

Question No : 101 - (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

Question No : 102 - (Topic 2)

Creating a secondary authentication process for network access would be an example of?

A. An administrator with too much time on their hands.
B. Putting undue time commitment on the system administrator.
C. Supporting the concept of layered security

D. Network segmentation.

Answer: C

Question No : 103 - (Topic 2)

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

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

Answer: D

Question No : 104 - (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

Question No : 105 - (Topic 2)

A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?

A. Have internal audit conduct another audit to see what has changed.
B. Contract with an external audit company to conduct an unbiased audit

C. Review the recommendations and follow up to see if audit implemented the changes
D. Meet with audit team to determine a timeline for corrections

Answer: C

Question No : 106 - (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

Question No : 107 - (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

Question No : 108 - (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

Question No : 109 - (Topic 2)

Which of the following are primary concerns for management with regard to assessing internal control objectives?

A. Confidentiality, Availability, Integrity
B. Compliance, Effectiveness, Efficiency
C. Communication, Reliability, Cost
D. Confidentiality, Compliance, Cost

Answer: B

Question No : 110 - (Topic 2)

Which of the following illustrates an operational control process:

A. Classifying an information system as part of a risk assessment
B. Installing an appropriate fire suppression system in the data center
C. Conducting an audit of the configuration management process
D. Establishing procurement standards for cloud vendors

Answer: B

Question No : 111 - (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

Question No : 112 - (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

Question No : 113 - (Topic 2)

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

A. Procedural control
B. Management control
C. Technical control
D. Administrative control

Answer: B

Question No : 114 - (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

Question No : 115 - (Topic 2)

IT control objectives are useful to IT auditors as they provide the basis for understanding the:

A. Desired results or purpose of implementing specific control procedures.
B. The audit control checklist.
C. Techniques for securing information.
D. Security policy

Answer: A

Question No : 116 - (Topic 2)

Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

A. Application logs
B. File integrity monitoring
C. SNMP traps
D. Syslog

Answer: B

Question No : 117 - (Topic 2)

The regular review of a firewall ruleset is considered a

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

Answer: A

Question No : 118 - (Topic 2)

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE	350-018 Dump PDF VCE	642-737 Dump PDF VCE	650-667 Dump PDF VCE
100-105 Dump PDF VCE	352-001 Dump PDF VCE	642-742 Dump PDF VCE	650-669 Dump PDF VCE
200-001 Dump PDF VCE	400-051 Dump PDF VCE	642-883 Dump PDF VCE	650-752 Dump PDF VCE
200-105 Dump PDF VCE	400-101 Dump PDF VCE	642-885 Dump PDF VCE	650-756 Dump PDF VCE
200-120 Dump PDF VCE	400-151 Dump PDF VCE	642-887 Dump PDF VCE	650-968 Dump PDF VCE
200-125 Dump PDF VCE	400-201 Dump PDF VCE	642-889 Dump PDF VCE	700-001 Dump PDF VCE
200-150 Dump PDF VCE	400-251 Dump PDF VCE	642-980 Dump PDF VCE	700-037 Dump PDF VCE
200-155 Dump PDF VCE	400-351 Dump PDF VCE	642-996 Dump PDF VCE	700-038 Dump PDF VCE
200-310 Dump PDF VCE	500-006 Dump PDF VCE	642-997 Dump PDF VCE	700-039 Dump PDF VCE
200-355 Dump PDF VCE	500-007 Dump PDF VCE	642-998 Dump PDF VCE	700-101 Dump PDF VCE
200-401 Dump PDF VCE	500-051 Dump PDF VCE	642-999 Dump PDF VCE	700-104 Dump PDF VCE
200-601 Dump PDF VCE	500-052 Dump PDF VCE	644-066 Dump PDF VCE	700-201 Dump PDF VCE
210-060 Dump PDF VCE	500-170 Dump PDF VCE	644-068 Dump PDF VCE	700-205 Dump PDF VCE
210-065 Dump PDF VCE	500-201 Dump PDF VCE	644-906 Dump PDF VCE	700-260 Dump PDF VCE
210-250 Dump PDF VCE	500-202 Dump PDF VCE	646-048 Dump PDF VCE	700-270 Dump PDF VCE
210-255 Dump PDF VCE	500-254 Dump PDF VCE	646-365 Dump PDF VCE	700-280 Dump PDF VCE
210-260 Dump PDF VCE	500-258 Dump PDF VCE	646-580 Dump PDF VCE	700-281 Dump PDF VCE
210-451 Dump PDF VCE	500-260 Dump PDF VCE	646-671 Dump PDF VCE	700-295 Dump PDF VCE
210-455 Dump PDF VCE	500-265 Dump PDF VCE	646-985 Dump PDF VCE	700-501 Dump PDF VCE
300-070 Dump PDF VCE	500-275 Dump PDF VCE	648-232 Dump PDF VCE	700-505 Dump PDF VCE
300-075 Dump PDF VCE	500-280 Dump PDF VCE	648-238 Dump PDF VCE	700-601 Dump PDF VCE
300-080 Dump PDF VCE	500-285 Dump PDF VCE	648-244 Dump PDF VCE	700-602 Dump PDF VCE
300-085 Dump PDF VCE	500-290 Dump PDF VCE	648-247 Dump PDF VCE	700-603 Dump PDF VCE
300-101 Dump PDF VCE	500-801 Dump PDF VCE	648-375 Dump PDF VCE	700-701 Dump PDF VCE
300-115 Dump PDF VCE	600-199 Dump PDF VCE	648-385 Dump PDF VCE	700-702 Dump PDF VCE
300-135 Dump PDF VCE	600-210 Dump PDF VCE	650-032 Dump PDF VCE	700-703 Dump PDF VCE
300-160 Dump PDF VCE	600-211 Dump PDF VCE	650-042 Dump PDF VCE	700-801 Dump PDF VCE
300-165 Dump PDF VCE	600-212 Dump PDF VCE	650-059 Dump PDF VCE	700-802 Dump PDF VCE
300-180 Dump PDF VCE	600-455 Dump PDF VCE	650-082 Dump PDF VCE	700-803 Dump PDF VCE
300-206 Dump PDF VCE	600-460 Dump PDF VCE	650-127 Dump PDF VCE	810-403 Dump PDF VCE
300-207 Dump PDF VCE	600-501 Dump PDF VCE	650-128 Dump PDF VCE	820-424 Dump PDF VCE
300-208 Dump PDF VCE	600-502 Dump PDF VCE	650-148 Dump PDF VCE	840-425 Dump PDF VCE
300-209 Dump PDF VCE	600-503 Dump PDF VCE	650-159 Dump PDF VCE	
300-210 Dump PDF VCE	600-504 Dump PDF VCE	650-281 Dump PDF VCE	
300-320 Dump PDF VCE	640-692 Dump PDF VCE	650-393 Dump PDF VCE	
300-360 Dump PDF VCE	640-875 Dump PDF VCE	650-472 Dump PDF VCE	
300-365 Dump PDF VCE	640-878 Dump PDF VCE	650-474 Dump PDF VCE	
300-370 Dump PDF VCE	640-911 Dump PDF VCE	650-575 Dump PDF VCE	
300-375 Dump PDF VCE	640-916 Dump PDF VCE	650-621 Dump PDF VCE	
300-465 Dump PDF VCE	642-035 Dump PDF VCE	650-663 Dump PDF VCE	
300-470 Dump PDF VCE	642-732 Dump PDF VCE	650-665 Dump PDF VCE	
300-475 Dump PDF VCE	642-747 Dump PDF VCE	650-754 Dump PDF VCE	