[May-2022 EC-COUNCIL 512-50 Official Cert Guide PDF [Q81-Q103

[May-2022] EC-COUNCIL 512-50 Official Cert Guide PDF
Exam 512-50: EC-Council Information Security Manager (E|ISM) - Actualtests4sure

Difficulty in writing 512-50 Exam

This is exam is very difficult for those candidates who don't practice during preparation and candidates need a lab for practicing. Then practical exposure is much required to understand the contents of the exam. So, if anyone is associated with some kinds of an organization where he has opportunities to practice but if you can't afford the lab and don't have time to practice. So, Actualtests4sure is the solution to this problem. We provide the best EC-Council 512-50 exam dumps and practice test for your preparation. EC-Council 512-50 exam dumps to ensure your success in the EC-Council Information Security Manager Certification Exam at first attempt. Our EC-Council 512-50 exam dumps are updated on regular basis. Actualtests4sure has the combination of PDF and VCE file that will be much helpful for candidates in passing the exam. Actualtests4sure provides verified questions with relevant answers which will be asked from candidates in their final exam. So, it makes it for candidates to get good grades in the final exam and one of the best features is we also provide **EC-Council 512-50 exam dumps** in PDF format which is candidates can download and study offline.

NEW QUESTION 81

Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?
* Risk Management
* Risk Assessment
* System Testing
* Vulnerability Assessment

NEW QUESTION 82

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

NEW QUESTION 83

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.

Which of the following is the FIRST action the CISO will perform after receiving the audit report?
* Inform peer executives of the audit results
* Validate gaps and accept or dispute the audit findings
* Create remediation plans to address program gaps
* Determine if security policies and procedures are adequate

NEW QUESTION 84

Which of the following is critical in creating a security program aligned with an organization’s goals?
* Ensure security budgets enable technical acquisition and resource allocation based on internal compliance requirements
* Develop a culture in which users, managers and IT professionals all make good decisions about information risk
* Provide clear communication of security program support requirements and audit schedules
* Create security awareness programs that include clear definition of security program goals and charters

NEW QUESTION 85

Which of the following is the MOST important reason for performing assessments of the security portfolio?
* To assure that the portfolio is aligned to the needs of the broader organization
* To create executive support of the portfolio
* To discover new technologies and processes for implementation within the portfolio
* To provide independent 3rd party reviews of security effectiveness

NEW QUESTION 86

When entering into a third party vendor agreement for security services, at what point in the process is it BEST to understand and validate the security posture and compliance level of the vendor?

* At the time the security services are being performed and the vendor needs access to the network
* Once the agreement has been signed and the security vendor states that they will need access to the network
* Once the vendor is on premise and before they perform security services
* Prior to signing the agreement and before any security services are being performed

NEW QUESTION 87

The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong?

(choose the BEST answer):
* Failed to identify all stakeholders and their needs
* Deployed the encryption solution in an inadequate manner
* Used 1024 bit encryption when 256 bit would have sufficed
* Used hardware encryption instead of software encryption

NEW QUESTION 88

The PRIMARY objective of security awareness is to:
* Ensure that security policies are read.
* Encourage security-conscious employee behavior.
* Meet legal and regulatory requirements.
* Put employees on notice in case follow-up action for noncompliance is necessary

NEW QUESTION 89

An organization information security policy serves to
* establish budgetary input in order to meet compliance requirements
* establish acceptable systems and user behavior
* define security configurations for systems
* define relationships with external law enforcement agencies

NEW QUESTION 90

Which represents PROPER separation of duties in the corporate environment?
* Information Security and Identity Access Management teams perform two distinct functions
* Developers and Network teams both have admin rights on servers
* Finance has access to Human Resources data
* Information Security and Network teams perform two distinct functions

NEW QUESTION 91

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.

What type of control is being implemented by supervisors and data owners?
* Management
* Operational
* Technical
* Administrative

NEW QUESTION 92

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.

The organization has already been subject to a significant amount of credit card fraud. Which of the following is the MOST likely reason for this fraud?
* Lack of compliance to the Payment Card Industry (PCI) standards
* Ineffective security awareness program
* Security practices not in alignment with ISO 27000 frameworks
* Lack of technical controls when dealing with credit card data

NEW QUESTION 93

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

Explanation

Scenario2

NEW QUESTION 94

The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:
* Contacting the Internet Service Provider for an IP scope
* Getting authority to operate the system from executive management
* Changing the default passwords
* Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

NEW QUESTION 95

Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?
* Trusted and untrusted networks
* Type of authentication

* Storage encryption
* Log retention

NEW QUESTION 96

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?
* Determine the risk tolerance
* Perform an asset classification
* Create an architecture gap analysis
* Analyze existing controls on systems

NEW QUESTION 97

When should IT security project management be outsourced?
* When organizational resources are limited
* When the benefits of outsourcing outweigh the inherent risks of outsourcing
* On new, enterprise-wide security initiatives
* On projects not forecasted in the yearly budget

NEW QUESTION 98

Which type of physical security control scan a person’s external features through a digital video camera before granting access to a restricted area?
* Iris scan
* Retinal scan
* Facial recognition scan
* Signature kinetics scan

NEW QUESTION 99

The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization’s
* Risk Management Program.
* Anti-Spam controls.
* Security Awareness Program.
* Identity and Access Management Program.

NEW QUESTION 100

The Information Security Governance program MUST:
* integrate with other organizational governance processes
* support user choice for Bring Your Own Device (BYOD)
* integrate with other organizational governance processes
* show a return on investment for the organization

NEW QUESTION 101

A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets. This demonstrates which of the following principles?

* Security alignment to business goals
* Regulatory compliance effectiveness
* Increased security program presence
* Proper organizational policy enforcement

NEW QUESTION 102

When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?
* Transfer financial resources from other critical programs
* Take the system off line until the budget is available
* Deploy countermeasures and compensating controls until the budget is available
* Schedule an emergency meeting and request the funding to fix the issue

NEW QUESTION 103

Which of the following most commonly falls within the scope of an information security governance steering committee?
* Approving access to critical financial systems
* Developing content for security awareness programs
* Interviewing candidates for information security specialist positions
* Vetting information security policies