712-50 Valid Mock Test & 712-50 Latest Test Format

BTW, DOWNLOAD part of BootcampPDF 712-50 dumps from Cloud Storage: https://drive.google.com/open?id=1I00Ic6x1tnQ5wFQJUJnTGTGrOelqgKMl

People who want to pass the exam have difficulty in choosing the suitable 712-50 study materials. They do not know which study materials are suitable for them, and they do not know which the study materials are best. Our company can promise that the 712-50 Study Materials from our company are best among global market. As is known to us, the 712-50 study materials from our company are the leading practice materials in this dynamic market.

EC-COUNCIL 712-50 Exam Syllabus Topics:

Topic	Details
Topic 1	• Compliance: This exam section covers evaluating external regulations, best practices, and rules to maintain security standards.
Topic 2	• Security, Program Management, and Operations: This section of the exam covers security program management and managing security program operations.

Topic 3	• Risk Management: This section covers building a risk management plan, assessing risks, building risk reports, and managing risk registers.
Topic 4	• Strategic Planning, Finance, Procurement, and Third-party Management: This section covers strategic planning, finance, and budget of the security department, and third-party management.

>> 712-50 Valid Mock Test <<

EC-COUNCIL 712-50 Latest Test Format & Reliable 712-50 Exam Labs

Being anxious for the exam ahead of you? Have a look of our 712-50 practice materials please. Presiding over the line of 712-50 practice materials over ten years, our experts are proficient as elites who made our 712-50 practice materials, and it is their job to officiate the routines of offering help for you. All points are predominantly related with the exam ahead of you. Every page is full of well-turned words for your reference related wholly with the real exam.

The CCISO certification exam is specifically designed for information security professionals who are responsible for the strategic planning, implementation, and management of an organization's information security program. 712-50 Exam Tests candidates on their knowledge of various domains, including governance and risk management, security program management, security operations and incident response, and information security core concepts.

EC-COUNCIL EC-Council Certified CISO (CCISO) Sample Questions (Q213-Q218):

NEW QUESTION # 213
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

Explanation:
Overview of ISO-22301:ISO-22301 is the international standard for Business Continuity Management Systems (BCMS), providing a framework for ensuring continuity and disaster recovery.
Why This Standard is Best:
* Offers specific guidance for developing and implementing consistent disaster recovery and business continuity processes.
* Focuses on resilience, recovery, and business continuity across diverse business units.
Why Other Options Are Incorrect:
* B. ITIL: Addresses IT service management, not business continuity.
* C. PCI-DSS: Focuses on payment card security, not continuity.
* D. ISO-27005: Focuses on risk management, not disaster recovery or business continuity.
References:EC-Council recognizes ISO-22301 as the leading standard for creating robust disaster recovery and business continuity frameworks.

NEW QUESTION # 214
Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

- A. Checking vendor product releases
- B. Performing system scans
- C. Auditing configuration templates
- D. Reviewing system administrator logs

Answer: B

Explanation:
To effectively identify technical vulnerabilities, system scans are among the most effective methods. These scans can automatically detect security weaknesses in software, configurations, and systems. Tools like vulnerability scanners perform automated checks against databases of known vulnerabilities, ensuring comprehensive coverage across IT environments. While reviewing logs, auditing templates, and checking vendor releases contribute to overall security, scanning is both systematic and thorough in identifying vulnerabilities.
Reference: EC-Council CISO training materials on technical assessments and vulnerability scanning techniques.

NEW QUESTION # 215
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. Forcing password changes every 90 days
- B. Professional user education on phishing conducted by a reputable vendor
- C. Multi-factor authentication employing hard tokens
- D. Decreasing the number of employees with administrator privileges

Answer: C

NEW QUESTION # 216
A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state.
Which of the following security issues is the MOST likely reason leading to the audit findings?

- A. Lack of proper access controls
- B. Lack of asset management processes
- C. Lack of hardening standards
- D. Lack of change management processes

Answer: D

Explanation:
Explanation of Issue:
* Change management processes ensure that updates and configuration changes to systems are documented, reviewed, and approved. The absence of such processes can lead to insecure configurations over time.
* This could include unauthorized changes, missed updates, or deviations from the originally hardened state.
Why Other Options Are Less Likely:
* A. Lack of asset management processes: This deals with inventory and tracking of assets rather than configuration changes.
* C. Lack of hardening standards: The system was initially hardened, so standards were likely in place.
* D. Lack of proper access controls: While important, this is unrelated to the system's deviation from the hardened state.
EC-Council CISO Reference:
The CISO program emphasizes the critical role of change management in maintaining secure configurations and compliance over time.

NEW QUESTION # 217
An organization's Information Security Policy is of MOST importance because

- A. it establishes a framework to protect confidential information
- B. it is formally acknowledged by all employees and vendors
- C. it communicates management's commitment to protecting information resources
- D. it defines a process to meet compliance requirements

Answer: C