

Our 712-50 study materials selected the most professional team to ensure that the quality of the 712-50 learning guide is all

In addition to passing the CCISO certification exam, candidates must also complete an application process that includes submitting a detailed resume, a job description, and a personal statement outlining their experience and qualifications. Once the application is approved, candidates will receive their CCISO certification and become part of an elite community of information security professionals.

We provide varied functions to help the learners learn our 712-50 study materials and prepare for the exam. The self-learn

We provide varied functions to help the learners learn our 712-50 study materials and prepare for the exam. The self-learning and

self-evaluation functions of our 712-50 exam questions help the learners check their learning results and the statistics and report functions help the learners find their weak links and improve them promptly. And you will be more confident as you know the information of the 712-50 Exam and the questions and answers.

The EC-Council Certified CISO (CCISO) certification is a globally recognized certification that is designed for those professionals who aspire to become a Chief Information Security Officer (CISO). EC-Council Certified CISO (CCISO) certification is intended to provide the necessary knowledge and skills to lead an organization's information security program. The CCISO certification is offered by the EC-Council, a leading organization in the information security industry.

EC-COUNCIL EC-Council Certified CISO (CCISO) Sample Questions (Q382-Q387):

NEW QUESTION # 382

Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus.

Which of the following phases in the incident handling process will utilize the signature to resolve this incident?

- A. Identification
- B. Recovery
- C. Containment
- **D. Eradication**

Answer: D

NEW QUESTION # 383

The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called

- A. Security accreditation
- **B. Security certification**
- C. Security system analysis
- D. Alignment with business practices and goals.

Answer: B

Explanation:

Definition of Security Certification Security certification is the systematic process of evaluating technical and non-technical security controls to ensure that an IT system meets specified security requirements. This process is a key step in validating the security posture of a system before deployment.

Purpose and Scope

* Technical Controls: Includes encryption, firewalls, access control mechanisms, etc.

* Non-Technical Controls: Policies, procedures, and organizational standards.

* Certification ensures that the implementation aligns with security frameworks and regulations.

Comparison of Options

* B. Security system analysis: A broader term for examining IT systems, not specifically tied to security requirement validation.

* C. Security accreditation: Focuses on management approval, which follows certification.

* D. Alignment with business practices and goals: Pertains to strategic alignment, not security validation.

EC-Council References

* Security certification aligns with phases of system development life cycles (SDLC) and is critical for ensuring compliance and risk management as per EC-Council CISO training.

NEW QUESTION # 384

Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.

When multiple regulations or standards apply to your industry you should set controls to meet the _____.

- **A. Easiest regulation or standard to implement**

- B. Recommendations of your Legal Staff
- C. Stricter regulation or standard
- D. Most complex standard

Answer: A

Explanation:
Explanation

NEW QUESTION # 385

The process of identifying and classifying assets is typically included in the

- A. Disaster Recovery plan
- B. Threat analysis process
- C. Business Impact Analysis
- D. Asset configuration management process

Answer: C

Explanation:

The process of identifying and classifying assets is integral to Business Impact Analysis (BIA) because it determines which assets are critical to the organization and how their loss would impact business operations.

This classification informs risk assessments, disaster recovery plans, and security prioritizations.

* Identification of Assets:

* Assets include hardware, software, data, and personnel. These are cataloged as part of the BIA to understand their role in business processes.

* Classification:

* Assets are classified based on criticality and sensitivity, considering how their compromise would affect confidentiality, integrity, or availability.

* Mapping Dependencies:

* BIA also involves mapping dependencies between assets and business processes to identify cascading impacts.

* Determining Impact:

* The financial, operational, legal, and reputational impact of asset loss or compromise is assessed.

* Foundation for Risk Mitigation:

* Asset classification through BIA forms the basis for prioritizing protective measures in disaster recovery and risk management.

* Risk and Business Impact: EC-Council emphasizes BIA as a cornerstone in identifying and safeguarding critical business functions and assets.

* Asset Management Framework: Proper classification under BIA supports alignment with cybersecurity frameworks like ISO 27001.

EC-Council CISO References:

NEW QUESTION # 386

What is the MOST important reason to have senior leadership endorse security policies?

- A. So they will accept ownership for security within the organization
- B. Auditors will recognize the organization's commitment to security
- C. So that they can be held legally accountable when a severe incident occurs
- D. To force employees to adhere to security policies

Answer: A

Explanation:

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

CCISO documentation stresses that policy endorsement by senior leadership establishes ownership and accountability. When executives formally endorse policies, security becomes an organizational responsibility rather than a technical one.

While enforcement and audit recognition are benefits, CCISO materials emphasize that endorsement ensures leadership accepts responsibility for risk decisions and supports enforcement across the enterprise.

• • • • •

- P.S. Free & New 712-50 dumps are available on Google Drive shared by ExamPrepAway: <https://drive.google.com/open?id=1ONE3MdLb4LvhEwVHooihRlgn5-VeDYE1>

P.S. Free & New 712-50 dumps are available on Google Drive shared by ExamPrepAway: <https://drive.google.com/open?id=1ONE3MdLb4LvhEwVHooihRlgn5-VeDYE1>