712-50 Study Plan | Reliable 712-50 Test Questions

BTW, DOWNLOAD part of Exam-Killer 712-50 dumps from Cloud Storage: https://drive.google.com/open?id=17Mz-TKil3QrTLbQ8_Sowq3yoZ-axLmIx

We not only do a good job before you buy our 712-50 test guides, we also do a good job of after-sales service. Because we are committed to customers who decide to choose our 712-50 study tool. We put the care of our customers in an important position. All customers can feel comfortable when they choose to buy our 712-50 study tool. We have specialized software to prevent the leakage of your information and we will never sell your personal information because trust is the foundation of cooperation between both parties. A good reputation is the driving force for our continued development. Our company has absolute credit, so you can rest assured to buy our 712-50 test guides.

The EC-Council Certified CISO (CCISO) is a professional certification program that is designed to recognize individuals who have demonstrated their proficiency and expertise in the field of information security. EC-Council Certified CISO (CCISO) certification program is offered by the EC-COUNCIL and is the first of its kind in the industry. The CCISO certification is globally recognized and is targeted at professionals who are responsible for overseeing the information security operations of an organization.

>> 712-50 Study Plan <<

Reliable 712-50 Test Questions & 712-50 Real Question

The EC-Council Certified CISO (CCISO) (712-50)questions are in use by many customers currently, and they are preparing for their best future daily. Even the students who used it in the past to prepare for the EC-COUNCIL 712-50 Certification Exam have rated our practice questions as one of the best. You will receive updates till 365 days after your purchase, and there is a 24/7 support system that assists you whenever you are stuck in any problem or issues.

712-50 Exam topics

Candidates must know the exam topics before they start of preparation. Because it will really help them in hitting the core. Our **712-50 exam dumps** will include the following topics:

- Governance and Risk Management (Policy, Legal, and Compliance) 17%
- Information Security Controls, Compliance, and Audit Management 19%

- Security Program Management & Operations 22%
- Information Security Core Competencies 25%
- Strategic Planning, Finance, Procurement, and Vendor Management 17%

EC-COUNCIL EC-Council Certified CISO (CCISO) Sample Questions (Q84-Q89):

NEW QUESTION # 84
IT control objectives are useful to IT auditors as they provide the basis for understanding the:

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

Answer: D

NEW QUESTION # 85
Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

- A. Planning
- B. System testing
- C. Incident response
- D. Risk assessment

Answer: B

NEW QUESTION # 86
The general ledger setup function in an enterprise resource package allows for setting accounting periods.
Access to this function has been permitted to users in finance, the shipping department, and production scheduling.
What is the most likely reason for such broad access?

- A. The need to create and modify the chart of accounts and its allocations.
- B. The lack of policies and procedures for the proper segregation of duties.
- C. The need to change accounting periods on a regular basis.
- D. The requirement to post entries for closed accounting period.

Answer: B

NEW QUESTION # 87
During a cyber incident, which non-security personnel might be needed to assist the security team?

- A. Network engineer, help desk technician, system administrator
- B. Financial analyst, payroll clerk, HR manager
- C. CIO, CFO, CSO
- D. Threat analyst, IT auditor, forensic analyst

Answer: A

Explanation:
* Non-Security Personnel for Incident Response:
* Cyber incidents often require cross-functional collaboration. Non-security IT staff like network engineers, help desk technicians, and system administrators play critical roles in identifying, containing, and remediating incidents.
* Network engineers: Analyze and secure affected network segments.
* Help desk technicians: Handle end-user issues and initial incident reports.
* System administrators: Investigate and secure affected systems.

* Why Not Other Options:
* A: These are security personnel, not non-security staff.
* C: Executives like CIO, CFO, and CSO may oversee strategic responses but are not directly involved in technical containment.
* D: Financial and HR personnel are unrelated to technical incident resolution.
References:
* EC-Council CISO Handbook: Incident Response Team Composition and Roles.

NEW QUESTION # 88
When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

- A. Threat Level, Risk of Compromise, and Consequences of Compromise
- B. Risk Avoidance, Threat Level, and Consequences of Compromise
- C. Reputational Impact, Financial Impact, and Risk of Compromise
- D. Risk Transfer, Reputational Impact, and Consequences of Compromise

Answer: A

Explanation:
ECCouncil 712-50 : Practice Test

NEW QUESTION # 89
.....