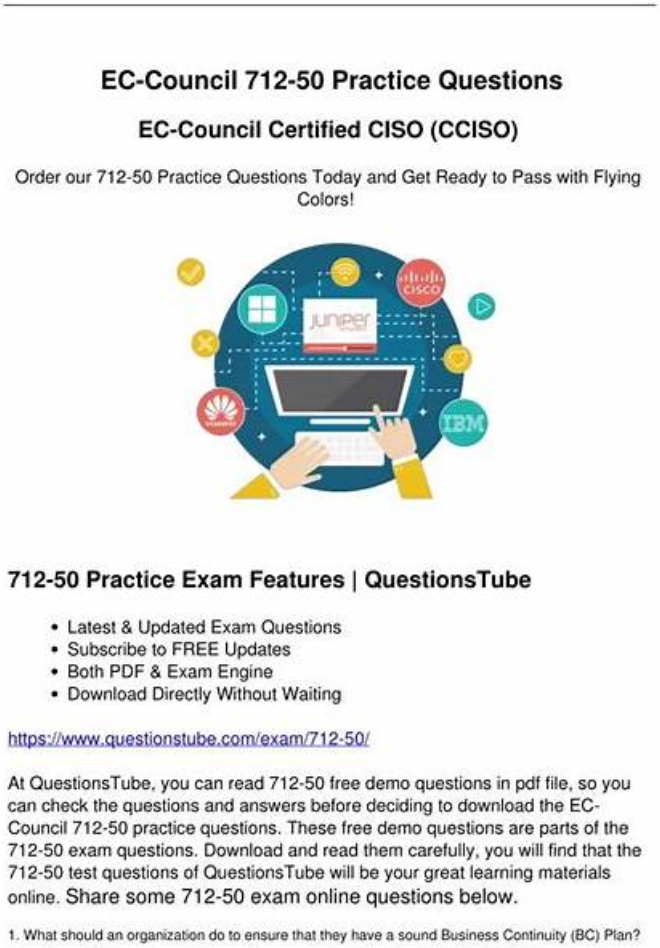
EC-COUNCIL 712-50 Latest Test Materials, Premium 712-50 Exam



EC-Council 712-50 Practice Questions

EC-Council Certified CISO (CCISO)

Order our 712-50 Practice Questions Today and Get Ready to Pass with Flying Colors!

712-50 Practice Exam Features | QuestionsTube

- Latest & Updated Exam Questions
- Subscribe to FREE Updates
- Both PDF & Exam Engine
- Download Directly Without Waiting

https://www.questionstube.com/exam/712-50/

At QuestionsTube, you can read 712-50 free demo questions in pdf file, so you can check the questions and answers before deciding to download the EC-Council 712-50 practice questions. These free demo questions are parts of the 712-50 exam questions. Download and read them carefully, you will find that the 712-50 test questions of QuestionsTube will be your great learning materials online. Share some 712-50 exam online questions below.

1. What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

P.S. Free & New 712-50 dumps are available on Google Drive shared by BraindumpStudy: https://drive.google.com/open?id=1kCozGh2Z3gi2ngNcD6A1Q1RrKkq8vqcM

Under the tremendous stress of fast pace in modern life, this version of our 712-50 test prep suits office workers perfectly. It can match your office software and as well as help you spare time practicing the 712-50 exam. As for its shining points, the PDF version can be readily downloaded and printed out so as to be read by you. It's really a convenient way for those who are fond of paper learning. With this kind of version, you can flip through the pages at liberty and quickly finish the check-up 712-50 Test Prep. What's more, a sticky note can be used on your paper materials, which help your further understanding the knowledge and review what you have grasped from the notes. While you are learning with our 712-50 quiz guide, we hope to help you make out what obstacles you have actually encountered during your approach for 712-50 exam torrent through our PDF version, only in this way can we help you win the 712-50 certification in your first attempt.

The EC-Council Certified CISO (CCISO) certification is a highly specialized and advanced certification that is designed to help information security professionals take their careers to the next level. EC-Council Certified CISO (CCISO) certification program is intended for experienced information security professionals who are looking to take on executive-level responsibilities in their organizations. The CCISO certification program is designed to test the knowledge, skills, and abilities of information security professionals in the areas of leadership, governance, strategic planning, and finance.

>> EC-COUNCIL 712-50 Latest Test Materials <<

100% Pass 2026 Professional EC-COUNCIL 712-50: EC-Council Certified CISO (CCISO) Latest Test Materials

We now live in a world which needs the talents who can combine the practical abilities and knowledge to apply their knowledge into the practical working conditions. To prove that you are that kind of talents you must boost some authorized and useful certificate and the test 712-50 certificate is one kind of these certificate. Passing the test 712-50 Certification can prove you are that kind of talents and help you find a good job with high pay and if you buy our 712-50 guide torrent you will pass the 712-50 exam successfully. And our pass rate of 712-50 exam prep is high as 99% to 100%.

EC-Council 712-50 Exam Syllabus Topics:

Topic	Details	Weightage
	1. Access Control • Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls and design an access control plan • Implement and manage an access control plan in alignment with the basic principles that govern the access control systems such as need-to-know • Identify different access control systems such as ID cards and biometrics • Understand the importance of warning banners for implementing access rules • Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the information systems **2. Social Engineering, Phishing Attacks, Identity Theft** • Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks • Design a response plan to identity theft incidences • Identify and design a plan to overcome phishing attacks **3. Physical Security** • Identify standards, procedures, directives, policies, regulations and laws for physical security • Determine the value of physical assets and the impact if unavailable • Identify resources needed to effectively implement a physical security plan • Design, implement and manage a coherent, coordinated, and holistic physical security plan to ensure overall organizational security • Establish objectives for personnel security to ensure alignment with overall security goals for the enterprise • Design and manage the physical security audit and update issues • Establish a physical security performance measurement system **4. Risk Management** • Identify the risk mitigation and risk treatment processes and understand the concept of acceptable risk • Identify resource requirements for risk management plan implementation • Design a systematic and structured risk assessment process and establish, in coordination with stakeholders, an IT security risk management program based on standards and procedures and ensure alignment with organizational goals and objectives • Develop, coordinate and manage risk management teams • Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals) • Develop an incident management measurement program and manage the risk management tools and techniques • Understand the residual risk in the information infrastructure • Assess threats and vulnerabilities to identify security risks, and regularly update applicable security controls	

- Identify changes to risk management policies and processes and ensure the risk management program remains current with the emerging risk and threat environment and in alignment with the organizational goals and objectives
- Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting

5. Disaster Recovery and Business Continuity Planning

- Develop, implement and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives
- Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities
- Identify the resources and roles of different stakeholders in business continuity programs
- Identify and prioritize critical business functions and consequently design emergency delegations of authority, orders of succession for key positions, the enterprise continuity of operations organizational structure and staffing model
- Direct contingency planning, operations, and programs to manage risk
- Understand the importance of lessons learned from test, training and exercise, and crisis events
- Design documentation process as part of the continuity of operations program
- Design and execute a testing and updating plan for the continuity of operations program
- Understand the importance of integration of IA requirements into the Continuity of Operations Plan (COOP).
- Identify the measures to increase the level of emergency preparedness such as backup and recovery solutions and design standard operating procedures for implementation during disasters

6. Firewall, IDS/IPS and Network Defense Systems

- Identify the appropriate intrusion detection and prevention systems for organizational information security
- Design and develop a program to monitor firewalls and identify firewall configuration issues
- Understand perimeter defense systems such as grid sensors and access control lists on routers, firewalls, and other network devices
- Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security
- Understand the concept of network segmentation
- Manage DMZs, VPN and telecommunication technologies such as PBX and VoIP
- Identify network vulnerabilities and explore network security controls such as use of SSL and TLS for transmission security
- Support, monitor, test, and troubleshoot issues with hardware and software
- Manage accounts, network rights, and access to systems and equipment

7. Wireless Security

- Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools

8. Virus, Trojans and Malware Threats

- Assess the threat of virus, Trojan and malware to organizational security and identify sources and mediums of malware infection
- Deploy and manage anti-virus systems
- Develop process to counter virus, Trojan, and malware threats

9. Secure Coding Best Practices and Securing Web Applications

- Develop and maintain software assurance programs in alignment with the secure coding principles and each phase of System Development Life Cycle (SDLC)
- Understand various system-engineering practices
- Configure and run tools that help in developing secure programs

Information Security Core Competencies	• Understand the software vulnerability analysis techniques • Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards • Identify web application vulnerabilities and attacks and web application security tools to counter attacks **10. Hardening OS** • Identify various OS vulnerabilities and attacks and develop a plan for hardening OS systems • Understand system logs, patch management process and configuration management for information system security **11. Encryption Technologies** • Understand the concept of encryption and decryption, digital certificates, public key infrastructure and the key differences between cryptography and steganography • Identify the different components of a cryptosystem • Develop a plan for information security encryption techniques **12. Vulnerability Assessment And Penetration Testing** • Design, develop and implement a penetration testing program based on penetration testing methodology to ensure organizational security • Identify different vulnerabilities associated with information systems and legal issues involved in penetration testing • Develop pre and post testing procedures • Develop a plan for pen test reporting and implementation of technical vulnerability corrections • Develop vulnerability management systems **13.Computer Forensics and Incident Response** • Develop a plan to identify a potential security violation and take appropriate action to report the incident • Comply with system termination procedures and incident reporting requirements related to potential security incidents or actual breaches • Assess potential security violations to determine if the network security policies have been breached, assess the impact, and preserve evidence • Diagnose and resolve IA problems in response to reported incidents • Design incident response procedures • Develop guidelines to determine whether a security incident is indicative of a violation of law that requires specific legal action • Identify the volatile and persistent system information • Set up and manage forensic labs and programs • Understand various digital media devices, e-discovery principles and practices and different file systems • Develop and manage an organizational digital forensic program • Establish, develop and manage forensic investigation teams • Design investigation processes such as evidence collection, imaging, data acquisition, and analysis • Identify the best practices to acquire, store and process digital evidence • Configure and use various forensic investigation tools • Design anti-forensic techniques	25%

Security Program Management & Operations	- For each information systems project develop a clear project scope statement in alignment with organizational objectives - Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan - Develop, manage and monitor the information systems program budget, estimate and control costs of individual projects - Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program (e.g., people, infrastructure, and architecture) - Acquire, develop and manage information security project team - Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability - Direct information security personnel and establish communications, and team activities, between the information systems team and other security-related personnel (e.g., technical support, incident management, security engineering) - Resolve personnel and teamwork issues within time, cost, and quality constraints - Identify, negotiate and manage vendor agreement and community - Participate with vendors and stakeholders to review/assess recommended solutions; identify incompatibilities, challenges, or issues with proposed solutions - Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization - Develop a plan to continuously measure the effectiveness of the information systems projects to ensure optimal system performance - Identify stakeholders, manage stakeholders' expectations and communicate effectively to report progress and performance - Ensure that necessary changes and improvements to the information systems processes are implemented as required	22%
Governance and Risk Management (Policy, Legal, and Compliance)	- Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.- Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards and policies. - Establish information security management structure. - Establish a framework for information security governance monitoring (considering cost/benefits analyses of controls and ROI). - Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program. - Understand the enterprise information security compliance program and manage the compliance team. - Analyze all the external laws, regulations, standards, and best practices applicable to the organization. - Understand the various provisions of the laws that affect the organizational security such as Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act [HIPAA], Federal Information Security - Management Act [FISMA], Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc. - Be familiar with the different standards such as ISO 27000 series, Federal Information Processing Standards [FIPS] - Understand the federal and organization specific published documents to manage operations in a computing environment - Assess the major enterprise risk factors for compliance - Coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk - Understand the importance of regulatory information security organizations and appropriate industry groups, forums, and stakeholders - Understand the information security changes, trends, and best practices -Manage enterprise compliance program controls - Understand the information security compliance process and procedures -Compile, analyze, and report compliance programs - Understand the compliance auditing and certification programs -Follow organizational ethics	17%

Difficulty in writing 712-50 Exam

EC-Council Certified CISO Certification exam has a higher rank in the Information Technology sector. Candidate can add the most powerful EC-Council 712-50 certification on their resume by passing EC-Council 712-50 exam. EC-Council 712-50 is a very challenging exam Candidate will have to work hard to pass this exam. With the help of BraindumpStudy provided the right focus and preparation material passing this exam is an achievable goal. BraindumpStudy provide the most relevant and updated **EC-Council 712-50 exam dumps**. Furthermore, We also provide the EC-Council 712-50 practice test that will be much beneficial in the preparation. Our aims to provide the best **EC-Council 712-50 pdf exam dumps**. We are providing all useful preparation materials such as EC-Council 712-50 exam dumps that had been verified by the EC-Council experts, EC-Council 712-50 braindumps and customer care service in case of any problem. These are things are very helpful in passing the exam with good grades.

EC-COUNCIL EC-Council Certified CISO (CCISO) Sample Questions (Q131-Q136):

NEW QUESTION # 131
When you develop your audit remediation plan what is the MOST important criteria?

- A. To validate the remediation process with the auditor.
- B. To remediate half of the findings before the next audit.
- C. To remediate all of the findings before the next audit.
- D. To validate that the cost of the remediation is less than the risk of the finding.

Answer: D

Explanation:
Importance of Cost-Risk Analysis
* The EC-Council CISO framework emphasizes the principle of risk-based decision-making in all cybersecurity processes, including audit remediation. Addressing audit findings requires organizations to evaluate the potential risks associated with each finding and prioritize remediation efforts based on their cost-effectiveness.
* Ensuring that the cost of remediation is proportional to the risk mitigated avoids unnecessary expenditures while addressing critical vulnerabilities.
Comparison with Other Options
* A. To remediate half of the findings before the next audit:This approach lacks a strategic foundation.
Arbitrarily remediating half of the findings does not align with a risk-based strategy, leading to potential neglect of high-priority issues.
* B. To remediate all of the findings before the next audit:While remediating all findings is ideal, it is often impractical due to resource constraints. A prioritized, risk-based approach ensures critical vulnerabilities are addressed first, maximizing the impact of remediation efforts.
* D. To validate the remediation process with the auditor:Although validation with the auditor is a good practice, it is a secondary step. The primary focus must be on ensuring that remediation efforts align with risk mitigation objectives and resource efficiency.
EC-Council CISO Guidance on Audit Remediation Plans
* The framework highlights these critical steps:
* Risk Assessment: Analyze the severity and potential impact of findings.
* Cost-Benefit Analysis: Determine if the remediation cost is justified by the reduction in risk exposure.
* Prioritization: Address high-risk findings first, ensuring critical vulnerabilities are mitigated promptly.
* Alignment with Organizational Goals: Ensure remediation efforts support broader business and security objectives.
Balancing Compliance and Practicality
* An effective audit remediation plan balances compliance requirements with practical considerations.
Overcommitting resources to less impactful findings can divert attention from critical risks.
* Validating the cost-risk ratio ensures that resources are utilized effectively, enabling sustainable compliance and operational resilience.
Conclusion
* The most important criterion when developing an audit remediation plan is to validate that the cost of the remediation is less than the risk of the finding. This approach ensures that the organization prioritizes its efforts effectively, aligns with risk management principles, and maximizes resource utilization.

NEW QUESTION # 132
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?

- A. Administrative
- B. Technical
- C. Management
- D. Operational

Answer: A

Explanation:
The controls implemented by supervisors and data owners to vet and approve access are administrative controls, as they involve processes, policies, and personnel oversight.
* Definition of Administrative Controls:
* Focus on governance and procedural enforcement to manage access and mitigate risks.
* Examples: Access approval processes, training, and policies.
* Comparison with Other Controls:
* Management Controls: High-level oversight but less focused on operational processes.
* Operational Controls: Day-to-day activities but do not cover access approval.
* Technical Controls: Involve automated systems (e.g., firewalls, encryption) rather than human processes.
* Relevance to Scenario:
* Vetting and approval processes by supervisors and data owners are procedural, fitting within the administrative category.
* Access Control Best Practices: Highlights administrative controls as essential for ensuring appropriate access management.
* Security Governance Frameworks: Emphasizes the role of procedural controls in aligning access with business objectives.
EC-Council CISO References:

NEW QUESTION # 133
An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

- A. Operational Control
- B. Training Control
- C. Management Control
- D. Technical Control

Answer: B

Explanation:
Role of Security Awareness Training:
* Training controls enhance employees' ability to recognize and avoid sophisticated threats like spear phishing.
Effective Utilization:
* In this case, the employee's ability to avoid the attack demonstrates the success of the corporate information security awareness program.
Supporting Reference:
* CCISO materials emphasize the importance of training as a control to reduce human-related risks in security.

NEW QUESTION # 134
Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:

- A. Calculate annual loss expectancy
- B. Develop a cost-benefit analysis
- C. Create a detailed technical executive summary
- D. Create timelines for mitigation

Answer: B

Explanation:
When communicating security priorities in business terms, a cost-benefit analysis helps explain the value of information resources and justifies security expenditures effectively to executives.
* Understanding Executive Priorities:
* Executives focus on return on investment (ROI), cost efficiency, and alignment with business goals.
* Cost-Benefit Analysis:
* Quantifies the benefits of protecting an asset versus the cost of implementing controls.
* Provides actionable insights for decision-makers.
* Relevance of Other Options:
* Timelines and Executive Summaries do not provide the needed financial justification.
* Annual Loss Expectancy (ALE) is a metric but less comprehensive than a full cost-benefit analysis.
* Strategic Alignment: Emphasizes cost-benefit analysis for aligning security initiatives with business value.
* Risk Assessment and Prioritization: Stresses the need to communicate security impact in financial terms to executives.

NEW QUESTION # 135
What is the main purpose of the Incident Response Team?

- A. Provide current employee awareness programs
- B. Create effective policies detailing program activities
- C. Communicate details of information security incidents
- D. Ensure efficient recovery and reinstate repaired systems

Answer: D

NEW QUESTION # 136
.....