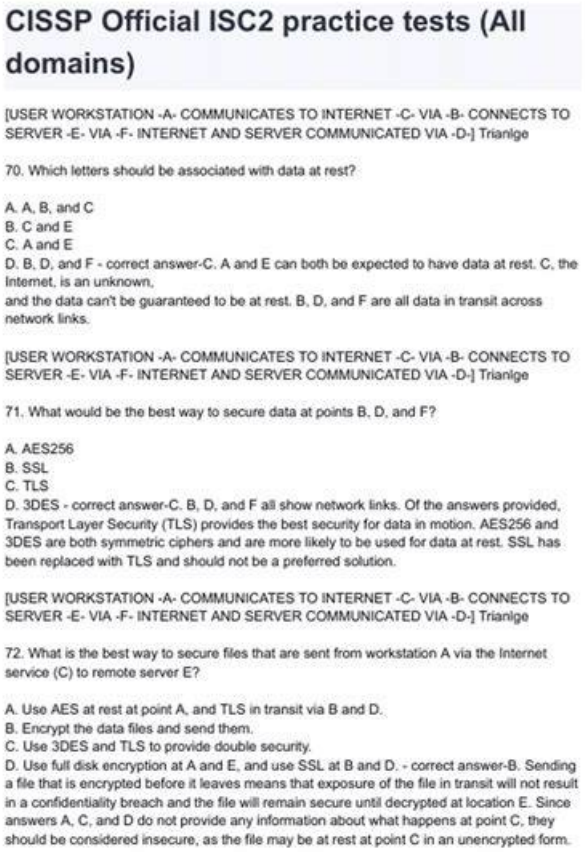
Most ISC CISSP Reliable Questions | Exam CISSP Actual Tests



CISSP Official ISC2 practice tests (All domains)

[USER WORKSTATION -A- COMMUNICATES TO INTERNET -C- VIA -B- CONNECTS TO SERVER -E- VIA -F- INTERNET AND SERVER COMMUNICATED VIA -D-] Trianlge

70. Which letters should be associated with data at rest?

A. A, B, and C
B. C and E
C. A and E
D. B, D, and F - correct answer-C. A and E can both be expected to have data at rest. C, the Internet, is an unknown,
and the data can't be guaranteed to be at rest. B, D, and F are all data in transit across network links.

[USER WORKSTATION -A- COMMUNICATES TO INTERNET -C- VIA -B- CONNECTS TO SERVER -E- VIA -F- INTERNET AND SERVER COMMUNICATED VIA -D-] Trianlge

71. What would be the best way to secure data at points B, D, and F?

A. AES256
B. SSL
C. TLS
D. 3DES - correct answer-C. B, D, and F all show network links. Of the answers provided, Transport Layer Security (TLS) provides the best security for data in motion. AES256 and 3DES are both symmetric ciphers and are more likely to be used for data at rest. SSL has been replaced with TLS and should not be a preferred solution.

[USER WORKSTATION -A- COMMUNICATES TO INTERNET -C- VIA -B- CONNECTS TO SERVER -E- VIA -F- INTERNET AND SERVER COMMUNICATED VIA -D-] Trianlge

72. What is the best way to secure files that are sent from workstation A via the Internet service (C) to remote server E?

A. Use AES at rest at point A, and TLS in transit via B and D.
B. Encrypt the data files and send them.
C. Use 3DES and TLS to provide double security.
D. Use full disk encryption at A and E, and use SSL at B and D. - correct answer-B. Sending a file that is encrypted before it leaves means that exposure of the file in transit will not result in a confidentiality breach and the file will remain secure until decrypted at location E. Since answers A, C, and D do not provide any information about what happens at point C, they should be considered insecure, as the file may be at rest at point C in an unencrypted form.

P.S. Free 2026 ISC CISSP dumps are available on Google Drive shared by Pass4guide: https://drive.google.com/open?id=1Rs4A6hGxcu803GYHLvLkOR6Mx0TJ3utM

If you want to practice the CISSP exam questions with different eletronic devices. We believe our APP version of CISSP training braindump will be very convenient for you. In addition, the online version of our CISSP training materials can work in an offline state. If you buy our CISSP Study Guide, you have the chance to use our CISSP study materials for preparing your exam when you are in an offline state. We believe that you will like the online version of our CISSP exam questions.

ISC CISSP Exam Syllabus Topics:

Section	Weight	Objectives

Identity and Access Management	13%	- Manage identification and authentication • 1. MFA • 2. Federated identity - Control physical and logical access • 1. Identity lifecycle • 2. Access provisioning - Integrate identity as a service • 1. SSO • 2. Cloud identity

Security and Risk Management	15%	- Develop and manage security policies • 1. Policy lifecycle • 2. Standards and guidelines - Understand legal and regulatory issues • 1. Cyber crimes and data breaches • 2. Licensing and intellectual property - Establish and manage security awareness training • 1. Awareness programs • 2. Training effectiveness - Understand and apply threat modeling concepts • 1. Attack surfaces • 2. Threat actors - Apply supply chain risk management concepts • 1. Third-party governance • 2. Vendor assessments - Understand and apply security concepts • 1. Confidentiality, integrity and availability • 2. Due care and due diligence • 3. Security governance principles - Determine compliance requirements • 1. Legal and regulatory requirements • 2. Privacy requirements - Understand requirements for investigation types • 1. Criminal investigations • 2. Administrative investigations - Apply risk management concepts • 1. Risk treatment • 2. Risk assessment • 3. Risk monitoring - Evaluate and apply security governance principles • 1. Roles and responsibilities • 2. Security policies and procedures • 3. Organizational processes - Identify and analyze threats and vulnerabilities • 1. Threat modeling • 2. Risk analysis methodologies

Asset Security	10%	- Establish information handling requirements • 1. Secure disposal • 2. Data retention - Provision resources securely • 1. Media handling • 2. Asset lifecycle management - Manage data lifecycle • 1. Data storage • 2. Data sharing - Identify and classify information and assets • 1. Asset ownership • 2. Data classification
Communication and Network Security	13%	- Implement secure design principles in networks • 1. Network architecture • 2. Segmentation - Implement secure communication channels • 1. Secure protocols • 2. VPN - Secure network components • 1. Routers and switches • 2. Firewalls
Software Development Security	11%	- Identify and mitigate vulnerabilities • 1. Static and dynamic testing • 2. Code review - Understand software development lifecycle security • 1. DevSecOps • 2. Secure SDLC - Assess software security effectiveness • 1. Application testing • 2. Security metrics

Security Architecture and Engineering	13%	- Research and implement security models • 1. Trusted computing base • 2. Security frameworks - Understand security capabilities of systems • 1. Hardware security • 2. Virtualization - Select controls based on security requirements • 1. Preventive controls • 2. Detective controls - Apply cryptography • 1. PKI • 2. Encryption methods - Assess vulnerabilities of architectures • 1. Cloud-based systems • 2. Embedded systems
Security Assessment and Testing	12%	- Collect and analyze test outputs • 1. Reporting • 2. Log reviews - Conduct security control testing • 1. Vulnerability assessments • 2. Penetration testing - Design and validate assessment strategies • 1. Audit strategies • 2. Security testing
Security Operations	13%	- Implement incident management • 1. Incident response • 2. Recovery procedures - Conduct logging and monitoring activities • 1. SIEM • 2. Continuous monitoring - Implement disaster recovery processes • 1. Recovery testing • 2. Business continuity - Operate and maintain preventive measures • 1. Backup operations • 2. Patch management - Understand and support investigations • 1. Digital forensics • 2. Evidence handling

>> Most ISC CISSP Reliable Questions <<

Free PDF 2026 CISSP: Professional Most Certified Information Systems Security Professional (CISSP) Reliable Questions

Our customer service is available all day, and your problems can be solved efficiently at any time. Last but not least, we can guarantee the security of the purchase process of CISSP test questions and the absolute confidentiality of customer information. You do not have to worry about these issues, because we know that this is a basic condition for us to establish a good business model. At the same time, if you want to continue learning, CISSP Test Torrent will provide you with the benefits of free updates within one year and a discount of more than one year.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q339-Q344):

NEW QUESTION # 339
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

- A. Notify system and application owners.
- B. Document and verify the intrusion.
- C. Isolate and contain the intrusion.
- D. Apply patches to the Operating Systems (OS).

Answer: C

Explanation:
The first action for a security administrator who detects an intrusion on the network based on precursors and other indicators is to isolate and contain the intrusion. An intrusion is an unauthorized or malicious activity that attempts to compromise the security or the functionality of a system or a network. An intrusion can be detected by various methods, such as the analysis of the network traffic, the logs, the alerts, or the anomalies.
Precursors and indicators are the signs or the evidence of an intrusion or an attempted intrusion. Precursors are the events or the activities that occur before or during an intrusion, such as the reconnaissance, the scanning, or the probing. Indicators are the events or the activities that occur after or as a result of an intrusion, such as the exploitation, the backdoor, or the payload. The first action for a security administrator who detects an intrusion on the network is to isolate and contain the intrusion, which means to disconnect or block the affected system or network from the rest of the environment and prevent the intrusion from spreading or causing more damage.
Isolating and containing the intrusion can help protect the other systems or networks from being compromised, preserve the evidence for the investigation, and facilitate the recovery and the restoration of the normal operations. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 7: Security Operations, page
364. Free daily CISSP practice questions, Question 4.

NEW QUESTION # 340
Which of the following is not classified as "Security and Audit Frameworks and Methodologies"?

- A. Bell LaPadula
- B. IT Infrastructure Library (ITIL)
- C. Control Objectives for Information and related Technology (COBIT)
- D. Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Answer: A

Explanation:
Explanation/Reference:
Explanation:
The Bell-LaPadula model is a security model, not a Security and Audit Frameworks and Methodology. The Bell-LaPadula model is a subject-to-object model. An example would be how you (subject) could read a data element (object) from a specific database and write data into that database. The Bell-LaPadula model focuses on ensuring that subjects are properly authenticated-by having the necessary security clearance, need to know, and formal access approval-before accessing an object.

The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.
CobiT was derived from the COSO framework, developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission in 1985 to deal with fraudulent financial activities and reporting.
The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. ITIL is a customizable framework that is provided in a set of books or in an online format.
Incorrect Answers:
B: Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a Security and Audit Frameworks and Methodology.
C: IT Infrastructure Library (ITIL) is a Security and Audit Frameworks and Methodology.
D: Control Objectives for Information and related Technology (COBIT) is a Security and Audit Frameworks and Methodology.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 55-60, 369

NEW QUESTION # 341
Which access control method uses security policies and security awareness training to stop or deter an unauthorized activity from occurring?

- A. Corrective
- B. Authoritative
- C. Administrative
- D. Detective
- E. Preventative

Answer: E

Explanation:
Preventative access control is deployed to stop an unauthorized activity from occurring.

NEW QUESTION # 342
Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

- A. Ensure proper and identifiable data owners for each data element stored within an enterprise data lake.
- B. Ensure that any data passing within remit is being used in accordance with the rules and regulations of the business.
- C. Ensure adequate security controls applied to the enterprise data lake.
- D. Ensure proper business definition, value, and usage of data collected and stored within the enterprise data lake.

Answer: D

Explanation:
A data steward is responsible for ensuring the quality, consistency, and usability of data within an enterprise data lake. This includes defining the business context, purpose, and value of the data, as well as ensuring that the data is properly documented, classified, and governed. A data steward also facilitates the communication and collaboration between data producers, consumers, and owners within the organization. References:
* 1 (Domain 1: Security and Risk Management, Objective 1.5: Understand and apply concepts of data governance)
* 2 (Chapter 1: Security and Risk Management, Section 1.5.3: Data Governance)

NEW QUESTION # 343
Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

- A. A peer reviewer of the information security professional
- B. The information security professional who conducted the analysis
- C. The information security professional's supervisor
- D. Legal counsel for the information security professional's employer

Answer: B

Explanation:
Digital forensics is the process of collecting, preserving, analyzing, and presenting digital evidence from various sources, such as computers, networks, mobile devices, etc. The information security professional who conducted the analysis is the most qualified person to formulate conclusions from the digital forensic investigation, as they have the technical expertise, the knowledge of the case, and the familiarity with the evidence. The information security professional should also document their findings and methods in a clear and concise report that can be used for legal or administrative purposes.

NEW QUESTION # 344
.....

Our website can offer you the latest ISC pass guide and learning materials, which enable you pass CISSP valid exam at your first attempt. Besides, there are CISSP free braindumps that you can download to learn about our products. Once you decide to buy our test answers, you will be allowed to free update your CISSP Top Dumps one-year.