

# CISSP Trustworthy Source | CISSP Exam Discount



P.S. Free 2026 ISC CISSP dumps are available on Google Drive shared by Lead2Passed: <https://drive.google.com/open?id=1YmoYyXJF9qYCBjFPhiA4an1V2qp4PYK>

In addition, a 24/7 customer assistance is also available at CISSP to assist you in using the product during any technical hitch. In summary, getting ready for 60 certification test might be challenging, but with the appropriate strategy and our CISSP Actual Exam questions, you can clear the test in a short time.

## Elaborate the Format of the ISC CISSP Exam

The format of the ISC CISSP exam is:

- **Audio Questions:** Audio questions are presented in this section. The candidate will listen to English language questions and read the related information from a provided reference document.
- **Free Response:** The free-response section consists of one multiple-choice and three open-ended (short answer and essay questions).
- **Performance Exam:** This section includes performance tasks consisting of both open-ended and multiple-choice questions.

>> CISSP Trustworthy Source <<

## ISC CISSP Exam Discount - CISSP Sample Questions

Our CISSP training materials have been honored as the panacea for the candidates for the exam since all of the contents in the CISSP guide quiz are the essences of the exam. There are detailed explanations for some difficult questions in our CISSP exam practice. Consequently, with the help of our CISSP Study Materials, you can be confident that you will pass the exam and get the related certification as easy as rolling off a log. So what are you waiting for? Just take immediate actions!

## ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q566-Q571):

### NEW QUESTION # 566

Which of the following is MOST effective in quickly detecting malicious activity and reacting according to the inherent risk presented by potential rogue elements?

- A. Administer a Host-based Intrusion Detection System (HIS).
- B. Implement a tool based on data science and machine learning
- C. Conduct a manual audit of the audit logs
- **D. Implement a continuous monitoring program**

**Answer: D**

Explanation:

A continuous monitoring program is the most effective way to quickly detect malicious activity and respond based on the inherent risk. It provides real-time or near-real-time visibility into systems, networks, and applications, enabling organizations to promptly detect anomalies, policy violations, or threats.

### NEW QUESTION # 567

Which of the following is the BEST security practice for data stored in removable media and mobile devices

- A. Hash using the Message Digest 5 (MD5) algorithm
- B. Implement an Inventory control method
- C. Restrict access to information systems
- D. Encrypt using Advanced Encryption Standard (AES)

Answer: D

### NEW QUESTION # 568

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Access Control Model	Restrictions
Mandatory Access Control	End user cannot set controls
Discretionary Access Control (DAC)	Subject has total control over objects
Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
Rule based access control	Dynamically assigns roles to subjects based on criteria assigned by a custodian

Answer:

Explanation:

Access Control Model	Restrictions	
Mandatory Access Control	Mandatory Access Control	End user cannot set controls
Discretionary Access Control (DAC)	Discretionary Access Control (DAC)	Subject has total control over objects
Role Based Access Control (RBAC)	Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
Rule based access control	Rule based access control	Dynamically assigns roles to subjects based on criteria assigned by a custodian

### NEW QUESTION # 569

Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

- A. File hashing
- B. Storage encryption
- C. Data retention policy
- D. Data processing

Answer: A

### NEW QUESTION # 570

What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?

- A. The Reference Monitor
- B. The Security Domain
- C. The Trusted Computing Base
- D. The Security Kernel

**Answer: A**

Explanation:

Explanation/Reference:

Explanation:

The reference monitor refers to abstract machine that mediates all access to objects by subjects. This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor. In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are: The reference validation mechanism must always be invoked (complete mediation). Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy. The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced. The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced. For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide. The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim. According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.

Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept. The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects." The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct." The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy." The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group."

Incorrect Answers:

B: "The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.

C: "The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.

D: "The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.

References: Official ISC2 Guide to the CBK, page 324 AIO Version 3, pp. 272 - 274 AIOv4 Security Architecture and Design (pages 327 - 328) AIOv5 Security Architecture and Design (pages 330 - 331)

[https://en.wikipedia.org/wiki/Reference\\_monitor](https://en.wikipedia.org/wiki/Reference_monitor)

## NEW QUESTION # 571

.....

We are concerted company offering tailored services which include not only the newest and various versions of CISSP practice materials, but offer one-year free updates services with patient staff offering help 24/7. So there is considerate and concerted cooperation for your purchasing experience accompanied with patient staff with amity. Their enrichment is dependable and reliable. You can find CISSP practice materials on our official website we will deal with everything once your place your order.

**CISSP Exam Discount:** <https://www.lead2passed.com/ISC/CISSP-practice-exam-dumps.html>

- Pass CISSP Guide  CISSP Accurate Study Material  CISSP Valid Test Guide  Download ⇒ CISSP ⇐ for free

