CISSP

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 2088 questions + unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/cissp

$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 2088 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play

Practice Questions

Try all 30 first, then check the answer key at the back.

1. Which of the following access control models requires security clearance for subjects?

A. Discretionary access control
B. Identity-based access control
C. Role-based access control
D. Mandatory access control

2. In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

A. the access controls are often based on the individual's role or title within the organization
B. people need not use discretion
C. the access controls are not based on the individual's role or title within the organization
D. the access controls are based on the individual's role or title within the organization.

3. Which item is not part of a Kerberos authentication implementation?

A. Message authentication code
B. Authentication service
C. Ticket granting service
D. Users, programs, and services

**4. A central authority determines which files a user can access.

Which of the following best describes this?**

A. An access control list (ACL)
B. Discretionary access control model
C. An access control matrix
D. Nondiscretionary access control model

5. The major disadvantage of many Single Sign-On (SSO) implementations is described in which of the following?

A. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems
B. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
C. The initial logon process is cumbersome to discourage potential intruders.
D. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.

6. To computer security software, the three traditional methods of authenticating yourself are something you know, something you have, and something:

A. you are.
B. you read.
C. you do.
D. you need.

7. In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:

A. The individual's role in the organization
B. The group-dynamics as they relate to the individual's role in the organization
C. The society’s role in the organization
D. The group-dynamics as they relate to the master-slave role in the organization

8. In Mandatory Access Control, sensitivity labels attached to objects contain what information?

A. The items' need to know
B. The item's category
C. The item's classification and category set
D. The item's classification

**9. The Orange Book describes four hierarchical levels to categorize security systems.

Which of the following levels require mandatory protection?**

A. A, B, and C.
B. B and D.
C. A and B.
D. B and C.

10. As per the Orange Book, what are two types of system assurance?

A. Architectural Assurance and Implementation Assurance.
B. Design Assurance and Implementation Assurance.
C. Operational Assurance and Life-Cycle Assurance.
D. Operational Assurance and Architectural Assurance.

11. In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?

A. Take-Grant model
B. Access Matrix model
C. Biba model
D. Bell-LaPadula model

12. Of the following choices, what is not a valid security practice related to special privileges?

A. Monitor special privilege usage
B. Grant access to only trusted employees
C. Grant access equally to administrators and operators
D. Monitor special privilege assignments

13. Which of the following identifies vendor responsibilities and can include monetary penalties if the vendor doesn't meet the stated responsibilities?

A. Interconnection security agreement (ISA)
B. Memorandum of understanding (MOU)
C. Service level agreement (SLA)
D. Software as a Service (SaaS)

**14. The two main types of routing protocols are used to make routing decision based on either distance-vector routing protocols or link-state routing protocols. However, there are a handful of De facto and proprietary interior protocols in use.

Which De facto protocol uses link-state algorithms to send out routing table information?**

A. Routing Information Protocol
B. Interior Gateway Routing Protocol
C. None of the Above
D. Open Shortest Path First

15. What is needed to allow an external client to initiate a communication session with an internal system if the network uses a NAT proxy?

A. Reverse DNS
B. Static private IP address
C. IPSec tunnel
D. Static mode NAT

16. At which OSI model layer does the IPSec protocol function?

A. Session
B. Data Link
C. Transport
D. Network

17. Which of the following is a Bluetooth-based attack that relates to gaining unauthorized access through a Bluetooth connection?

A. Blue-access
B. Bluesnarfing
C. Blue-theft
D. Blue jacking

18. What block size is used by the Advanced Encryption Standard?

A. Variable
B. 64 bits
C. 128 bits
D. 32 bits

19. What is an advantage of RSA over DSA?

A. It employs a one-time encryption pad.
B. It uses fewer resources and encrypts faster because it uses symmetric keys.
C. It can provide digital signature and encryption functionality.
D. It is a block cipher rather than a stream cipher.

20. What TCP/IP communications port is used by Transport Layer Security traffic?

A. 559
B. 80
C. 220
D. 443

21. What is the most effective means of reducing the risk of losing the data on a mobile device, such as a notebook computer?

A. Encrypting the hard drive
B. Using a cable lock
C. Minimizing sensitive data stored on the mobile device
D. Defining a strong logon password

22. When evaluating safeguards, what is the rule that should be followed in most cases?

A. The annual costs of safeguards should equal the value of the asset.
B. The annual costs of safeguards should not exceed 10 percent of the security budget.
C. The annual costs of safeguards should not exceed the expected annual cost of asset loss.
D. The expected annual cost of asset loss should not exceed the annual costs of safeguards.

23. Who has the responsibility for providing reports to the senior management on the effectiveness of the security controls?

A. Information systems security professionals
B. Data custodians
C. Information systems auditors
D. Data owners

24. What law formalizes many licensing arrangements used by the software industry and attempts to standardize their use from state to state?

A. Uniform Computer Information Transactions Act
B. Digital Millennium Copyright Act
C. Gramm■Leach■Bliley Act
D. Computer Security Act

25. Normalizing data within a database could include all or some of the following except which one?

A. Eliminate duplicative columns from the same table.
B. Eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key
C. Eliminates Functional dependencies on non-key fields by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
D. Eliminating duplicate key fields by putting them into separate tables.

26. Which of the following are literal value placeholders in a Structured Query Language (SQL) query sent to a server's database?

A. Bind variables
B. Assimilation variables
C. Resolution variables
D. Reduction variables

27. Which is a critical component of database design that assures that attributes in a table are only part of the primary key?

A. Compaction
B. Normalization
C. Reduction
D. Assimilation

28. Concerning Application Control, which is NOT true?

A. It limits end users use of applications in such a way that only particular screens are visible.
B. Particular usage of the application can be recorded for audit purposes
C. Only specific records can be requested through the application controls
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

**29. Sara thinks that someone keeps trying to hack into her company's system and wants to know who and why. She decides to use a computer to set up a sacrificial lamb on the network.

What is Sara practicing?**

A. Statistical anomaly-based IDS
B. Host-based Detection
C. Honeypot
D. Network-based Detection

30. What type of interface testing would identify flaws in a program's command-line interface?

A. User interface testing
B. Security interface testing
C. Application programming interface testing
D. Physical interface testing

Answer Key & Explanations

1. D — Mandatory access control
Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.

2. D — the access controls are based on the individual's role or title within the organization.
With Non-Discretionary Access Control, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual’s role in the organization (role-based access control) or the subject’s responsibilities and duties (taskbased access control). In an organization where there are frequent personnel changes, non-discretionary access control is useful because the access controls are based on the individual’s role or title within the organization. These access controls do not need to be changed whenever a new person takes over that role.

3. A — Message authentication code
Message authentication code (MAC) is a cryptographic function and is not a key component of Kerberos. Kerberos is made up of a KDC, a realm of principals (users, services, applications, and devices), an authentication service, tickets, and a ticket granting service.

4. D — Nondiscretionary access control model
A nondiscretionary access control model uses a central authority to determine which objects (such as files) that users (and other subjects) can access. In contrast, a discretionary access control model allows users to grant or reject access to any objects they own. An ACL is an example or rule■based access control model. An access control matrix includes multiple objects, and it lists the subject’s access to each of the objects.

5. D — Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
Single Sign-On is a distributed Access Control methodology in which a user only has to authenticate once to have access to all major and secondary network domains.

When the individual needs extra resources, they would not be asked to re-authenticate. The security concern this raises is that if a fraudster is able to compromise those credentials, they will also have access to all the resources that the account has access to. Because they are distractors, all of the other responses are wrong.

6. A — you are.
Three common factors that can be used for authentication:

- Something a person knows.

- Something a person has.

- Something a person is.

7. A — The individual's role in the organization
With Non-Discretionary Access Control, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual’s role in the organization (role-based access control) or the subject’s responsibilities and duties (taskbased access control). In an organization where there are frequent personnel changes, non-discretionary access control is useful because the access controls are based on the individual’s role or title within the

organization. These access controls do not need to be changed whenever a new person takes over that role.

8. C — The item's classification and category set
Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc.) and a category (which is essentially an indication of the management level, department or project to which the object is available).Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects.

When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's credentials match the MAC security label properties of the object access is allowed. It is important to note that both the classification and categories must match. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

9. C — A and B.
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book.

TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels:

A. Verified protection

B. Mandatory protection

C. Discretionary protection

D. Minimal security

Classification A represents the highest level of assurance, and D represents the lowest level of assurance. Level B is the lowest level that requires mandatory protection. Level A, being a higher level also requires mandatory protection.

10. C — Operational Assurance and Life-Cycle Assurance.
When products are evaluated for the level of trust and assurance they provide, many times operational assurance and life-cycle assurance are part of the evaluation process. Operational assurance concentrates on the product’s architecture, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product. Examples of operational assurances examined in the evaluation process are access control mechanisms, the separation of privileged and user program code, auditing and monitoring capabilities, covert channel analysis, and trusted recovery when the product experiences unexpected circumstances. Life-cycle assurance pertains to how the product was developed and maintained. Each stage of the product’s life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product. Examples of life-cycle assurance standards are design specifications, clipping-level configurations, unit and integration testing, configuration management, and trusted distribution. Vendors looking to achieve one of the higher security ratings for their products will have each of these issues evaluated and tested.

11. D — Bell-LaPadula model
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The BellLaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject’s clearance is compared to the object’s classification and then specific rules are applied to control how subjectto-object interactions can take place. This model uses subjects, objects, access operations (read, write, and

read/write), and security levels. Subjects and objects can reside at different security levels and will have relationships and rules dictating the acceptable activities between them.

12. C — Grant access equally to administrators and operators
Special privileges should not be granted equally to administrators and operators. Instead, personnel should be granted only the privileges they need to perform their job. Special privileges are activities that require special access or elevated rights and permissions to perform administrative and sensitive job tasks. Assignment and usage of these privileges should be monitored, and access should be granted only to trusted employees.

13. C — Service level agreement (SLA)
A service level agreement identifies responsibilities of a third party such as a vendor and can include monetary penalties if the vendor doesn't meet the stated responsibilities. A MOU is in informal agreement and does not include monetary penalties. An ISA defines requirements for establishing, maintaining, and disconnecting a connection. SaaS is one of the cloud■based service models and does not specify vendor responsibilities.

14. D — Open Shortest Path First
Open Shortest Path First (OSPF) is a De facto protocol using link-state algorithms to send out routing table information. The use of algorithms allow for smaller, more frequent routing table updates to take place. This provides a more stable network than Routing Information Protocol, but requires more memory and CPU resources to support the extra processing. OSPF allows for a hierarchical routing network that has a backbone link connecting all subnets together.

15. D — Static mode NAT
Static mode NAT is needed to allow an outside entity to initiate communications with an internal system behind a NAT proxy.

16. D — Network
IPSec operates at the Network layer (layer 3).

17. B — Bluesnarfing
The attack that relates to gaining unauthorized access through a Bluetooth connection is a Bluesnarfing attack.

Bluesnarfing is the gaining of unauthorized access through a Bluetooth connection. This access can be gained through a phone, PDA, or any device using Bluetooth. Once access has been gained, the attacker can copy any data in the same way they would with any other unauthorized access. Blue jacking is the sending of unsolicited messages or spam over the Bluetooth connection.

18. C — 128 bits
The Advanced Encryption Standard uses a 128■bit block size, despite the fact that the Rijndael algorithm it is based on allows a variable block size.

19. C — It can provide digital signature and encryption functionality.
RSA can be used for data encryption, key exchange, and digital signatures. DSA can only be used for digital signatures.

20. D — 443
Transport Layer Security uses TCP port 443 for encrypted client■server communications.

21. C — Minimizing sensitive data stored on the mobile device
The risk of a lost or stolen notebook is the data loss, not the loss of the system itself. Thus, keeping minimal sensitive data on the system is the only way to reduce the risk. Hard drive encryption, cable locks, and strong passwords, although good ideas, are preventive tools, not means of reducing risk. They don't keep intentional and malicious data compromise from occurring; instead, they encourage honest people to stay honest.

22. C — The annual costs of safeguards should not exceed the expected annual cost of asset loss.
The annual costs of safeguards should not exceed the expected annual cost of asset loss.

23. C — Information systems auditors
The auditor who has responsibility for providing reports to the senior management on the effectiveness of the security controls.

The role of the auditor is to come around periodically and ensure you are doing what you are supposed to be doing. They make sure the correct controls are in place and are being maintained securely. The target of the auditor is to ensure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/or external auditors. The external auditors commonly work on behalf of a regulatory body to ensure compliance is being met.

24. A — Uniform Computer Information Transactions Act
The Uniform Computer Information Transactions Act (UCITA) attempts to implement a standard framework of laws regarding computer transactions to be adopted by all states. One of the issues addressed by UCITA is the legality of various types of software license agreements.

25. D — Eliminating duplicate key fields by putting them into separate tables.
Normalizing data within a database does not eliminate duplicate key fields by putting them into separate tables.

26. A — Bind variables
Bind variables as placeholders for literal values in a Structured Query Language (SQL) query sent to a server's database. The SQL statement is sent to the server for parsing, and the subsequent values are bound to the placeholders and delivered to the server separately. The term bind variable comes from this separate step.

27. B — Normalization
The first normal form (1NF) requires the creation of separate tables for each collection of related data and the identifying of each row by a unique column known as the primary key. The second normal form (2NF) requires the transfer of data that is only partially dependent on the main key to a different table. The third normal form (3NF) requires the elimination of data that does not rely only on the primary key. The process of conforming to the normal form is called normalization.

28. D — It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved
Application control limits what users can see or do within the application. For example, if a user does not have the necessary access privilege to perform some functions, the functions can be hidden from the screen or the screen itself can be hidden so the user cannot select it within the application. In a similar way, only the records a user has access to can be displayed.

What users may see and do within the application is limited by application control. For example, if a user lacks the necessary access privileges to execute some functions, the functions can be hidden from the screen, or the screen itself can be hidden so the user cannot choose it inside the program. Similarly, just the records that a user has access to are displayed.

29. C — Honeypot
When a company decides to use a computer to set up a sacrificial lamb on a network, they are creating a honeypot. This is to entice a would-be attacker to this computer instead of attacking authentic production systems on a network. The honeypot contains no real company information and thus will not be at risk if and when it is attacked. It also enables the administrator to know when certain types of attacks are happening so the environment can be fortified to track down the attacker.

30. A — User interface testing
User interface testing includes assessments of both graphical user interfaces (GUIs) and command■line interfaces (CLIs) for a software program.

Ready to pass?

Unlock the full CISSP bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/cissp

Also on iOS & Android — search your exam name on the App Store or Google Play