

ISC Practice Questions

Olivia Anderson · True North Accounting & Business Solutions · Study notes for educational use. Always confirm details against the current AICPA Blueprints and authoritative standards.

Twenty-five exam-style multiple-choice questions weighted like the ISC blueprint: information systems and data management, security and privacy, then SOC engagements. Give yourself about 1.5 minutes per question.

Area I: Information Systems and Data Management

Question 1 · Easy

Which is an example of infrastructure as a service (IaaS)?

- A. A cloud CRM application
- B. A web-based office productivity suite
- C. Virtual servers rented from a cloud provider
- D. Hosted email

Answer: C. With IaaS, the customer rents servers, storage and networking and manages the operating system, applications and data. A, B and D are software as a service, where the customer manages only its data and user access.

Question 2 · Medium

Which ACID property ensures that either all changes in a transaction are committed or none are?

- A. Consistency
- B. Atomicity
- C. Isolation
- D. Durability

Answer: B. Atomicity is all or nothing. A transfer's debit and credit both succeed or both roll back. Consistency keeps the database in a valid state, isolation keeps concurrent transactions from interfering, and durability makes committed changes permanent.

Question 3 · Medium

A company wants a recovery site that's fully equipped with hardware and current data and can take over almost immediately. Which should it choose?

- A. Cold site
- B. Warm site
- C. Reciprocal agreement with another company
- D. Hot site

Answer: D. A hot site is fully equipped with replicated data and supports a very low recovery time objective, at the highest cost. A warm site is partly equipped and takes longer, and a cold site provides only space and utilities.

Question 4 · Medium

Which backup strategy gives the fastest backups but the slowest restores?

- A. Full backups only
- B. A full backup plus incremental backups
- C. A full backup plus differential backups
- D. Mirroring

Answer: B. Incremental backups copy only changes since the last backup of any kind, so they're quick. Restoring requires the full backup plus every incremental in sequence. Differential backups copy changes since the last full backup, so restoring needs only the full backup and the latest differential.

Question 5 · Easy

In a three-tier architecture, which tier contains the application server and business logic?

- A. Presentation tier
- B. Application tier
- C. Data tier
- D. Physical tier

Answer: B. The presentation tier is the user interface, the application tier processes requests with business logic, and the data tier holds the database. Separating tiers improves scalability and security.

Question 6 · Medium

RAID 5 provides fault tolerance through:

- A. Mirroring all data
- B. Striping without redundancy

- C. Mirroring and striping combined
- D. Striping with parity

Answer: D. RAID 5 distributes data and parity across the drives, so it can rebuild after losing one drive. RAID 0 is striping with no redundancy, RAID 1 is mirroring and RAID 10 combines mirroring and striping.

Question 7 · Medium

Compared with relational databases, NoSQL databases typically:

- A. Require a fixed schema
- B. Use SQL as their only query language
- C. Scale horizontally more easily
- D. Guarantee ACID transactions in all cases

Answer: C. NoSQL databases use flexible schemas and scale out by adding servers. Many favor availability and eventual consistency over strict ACID guarantees. Relational databases use fixed schemas and SQL.

Question 8 · Easy

What does a recovery point objective (RPO) measure?

- A. How quickly systems must be restored
- B. The maximum acceptable data loss, measured in time
- C. The longest the business can survive an outage
- D. The cost of disaster recovery

Answer: B. An RPO of four hours means losing up to four hours of data is acceptable, which drives backup frequency. A describes the recovery time objective, and C describes maximum tolerable downtime.

Area II: Security, Confidentiality and Privacy

Question 9 · Medium

Which is a preventive control?

- A. Reconciling the bank statement
- B. Reviewing exception reports
- C. Requiring strong passwords with MFA
- D. Reviewing log files

Answer: C. Preventive controls stop problems before they happen, such as authentication, access controls, segregation of duties and firewalls. A, B and D are detective controls that find problems after they occur.

Question 10 · Easy

What does the C in the CIA triad stand for?

- A. Compliance
- B. Confidentiality
- C. Control
- D. Cryptography

Answer: B. The triad is confidentiality (only authorized users can access information), integrity (information is accurate and unaltered) and availability (information is accessible when needed).

Question 11 · Medium

A company requires a password and a fingerprint scan to log in. Which authentication factors are used?

- A. Two factors from the same category
- B. Something you have and something you are
- C. Something you know and something you have
- D. Something you know and something you are

Answer: D. A password is something you know, and a fingerprint is something you are. MFA requires factors from two or more different categories.

Question 12 · Medium

Under GDPR, how long does an organization generally have to notify the supervisory authority after becoming aware of a personal data breach?

- A. 24 hours
- B. 72 hours
- C. Five business days
- D. 30 days

Answer: B. The deadline is 72 hours, where feasible. Affected individuals must be told without undue delay when the breach is likely to result in a high risk to them. For comparison, HIPAA requires notice to individuals within 60 days of discovery.

Question 13 · Easy

Which method uses the same key for encryption and decryption?

- A. Asymmetric encryption
- B. Public key encryption
- C. Hashing
- D. Symmetric encryption

Answer: D. Symmetric encryption, such as AES, is fast but requires sharing the key securely. Asymmetric encryption uses a public and private key pair, such as RSA, and is often used to exchange symmetric keys. Hashing is one-way and can't be decrypted.

Question 14 · Medium

Which firewall tracks the state of network connections and makes decisions based on the context of traffic?

- A. Stateful inspection firewall
- B. Packet-filtering firewall
- C. Application-level proxy
- D. Circuit-level gateway

Answer: A. A stateful firewall remembers connections and, for example, allows responses to outbound requests. Packet filters judge each packet alone. Proxies inspect application content, and next-generation firewalls add deep packet inspection and intrusion prevention.

Question 15 · Medium

Which access control model assigns permissions to job roles and then assigns users to those roles?

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

Answer: C. Role-based access control is the most common model in business. With discretionary access control the owner decides, with mandatory access control the system enforces labels and clearances, and attribute-based access control considers attributes such as time and location.

Question 16 · Easy

Encrypting a laptop's hard drive primarily protects which security objective if the laptop is stolen?

- A. Availability

- B. Integrity
- C. Confidentiality
- D. Nonrepudiation

Answer: C. Encryption keeps data unreadable without the key. Integrity is addressed with hashing and digital signatures, availability with backups and redundancy, and nonrepudiation with digital signatures.

Question 17 · Hard

A sender wants the recipient to be able to verify that a message came from the sender and wasn't altered. Which key does the sender use to create the digital signature?

- A. The sender's public key
- B. The recipient's public key
- C. The recipient's private key
- D. The sender's private key

Answer: D. The sender encrypts a hash of the message with the sender's private key. The recipient verifies it with the sender's public key. Encrypting with the recipient's public key provides confidentiality, not authentication.

Question 18 · Medium

Which function was added in NIST Cybersecurity Framework 2.0?

- A. Identify
- B. Recover
- C. Detect
- D. Govern

Answer: D. CSF 2.0 (2024) added Govern, covering cybersecurity strategy, policy, roles and supply chain risk, to the existing Identify, Protect, Detect, Respond and Recover functions.

Area III: Considerations for SOC Engagements

Question 19 · Medium

What is the main difference between a SOC 1 and a SOC 2 report?

- A. SOC 1 addresses controls relevant to user entities' financial reporting, and SOC 2 addresses the Trust Services Criteria
- B. SOC 1 is available only as Type 1, and SOC 2 can be Type 1 or Type 2

- C. SOC 1 is for public companies, and SOC 2 is for private companies
- D. SOC 1 always covers a longer period

Answer: A. SOC 1 serves user auditors in financial statement audits, for example for a payroll processor. SOC 2 covers security, availability, processing integrity, confidentiality and privacy for a broader set of users, such as a cloud provider's customers. Both can be Type 1 or Type 2.

Question 20 · Easy

In a SOC 1 Type 2 engagement, what does the service auditor's opinion cover?

- A. The fairness of the description only
- B. Operating effectiveness of controls only
- C. The fairness of the description, the suitability of design and the operating effectiveness of controls
- D. Only the controls of subservice organizations

Answer: C. A Type 1 report covers the description and suitability of design as of a date. A Type 2 report adds operating effectiveness throughout a period and includes a description of the tests performed and their results.

Question 21 · Hard

In a SOC 1 Type 2 engagement, the service auditor's tests find that a control didn't operate effectively during part of the period. What should the service auditor do?

- A. Withdraw from the engagement
- B. Omit the deviation if the control was fixed before the end of the period
- C. Describe the deviation in the tests and results section and consider whether the opinion should be modified
- D. Always issue an adverse opinion

Answer: C. Deviations are always described in the tests of controls and results. If they mean a control objective wasn't achieved, the service auditor modifies the opinion, typically with a qualified opinion. User auditors then decide how the deviation affects their reliance.

Question 22 · Medium

Which statement about complementary user entity controls (CUECs) is true?

- A. They're controls the service organization must implement
- B. They're optional controls that enhance security
- C. They apply only to SOC 2 reports
- D. They're controls the user entity must have for the control objectives or criteria to be achieved

Answer: D. The service organization's controls assume the user has certain controls, such as approving timesheets and reviewing payroll reports. CUECs appear in management's description and apply to both SOC 1 and SOC 2

reports.

Question 23 · Medium

Which Trust Services Criteria category addresses whether system processing is complete, valid, accurate, timely and authorized?

- A. Security
- B. Availability
- C. Processing integrity
- D. Confidentiality

Answer: C. Security, the common criteria, is included in every SOC 2. Availability, processing integrity, confidentiality and privacy are added depending on the services and users' needs.

Question 24 · Hard

A service organization uses a subservice organization and presents it under the carve-out method. Which statement is true?

- A. The service auditor tests controls at both organizations
- B. The service auditor must issue a qualified opinion
- C. The carve-out method isn't allowed in SOC 1 engagements
- D. The subservice organization's controls are excluded from the description and the service auditor's scope

Answer: D. Under carve-out, the description identifies the services the subservice organization performs but excludes its controls, so user auditors may need a separate report on it. Under the inclusive method, its controls are included and tested.

Question 25 · Medium

A service organization wants a report on its system that it can post on its website for anyone to read. Which report fits?

- A. SOC 1 Type 2
- B. SOC 2 Type 2
- C. SOC 3
- D. Agreed-upon procedures report

Answer: C. A SOC 3 report covers the Trust Services Criteria in a short, general-use report without detailed test results. SOC 1 and SOC 2 reports are restricted to specified users.

Answer Key

1. C	2. B	3. D	4. B	5. B
6. D	7. C	8. B	9. C	10. B
11. D	12. B	13. D	14. A	15. C
16. C	17. D	18. D	19. A	20. C
21. C	22. D	23. C	24. D	25. C

Scoring: 23–25 correct, you’re ready. 20–22, review the ones you missed. 17–19, more study on weak areas. Below 17, work back through the ISC study guide first.

If you’re struggling, focus on: SOC 1 vs. SOC 2 vs. SOC 3, Type 1 vs. Type 2, the Trust Services Criteria, cloud service models, the CIA triad and privacy laws (GDPR, CCPA, HIPAA).