

ISC Complete Study Guide

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

Information Systems and Controls, the discipline section for IT audit, cybersecurity and SOC reporting. Organized by the 2026 AICPA Blueprint.

AREA	TOPIC	WEIGHT
I	Information Systems and Data Management	35–45%
II	Security, Confidentiality and Privacy	35–45%
III	Considerations for System and Organization Controls (SOC) Engagements	15–25%

ISC leans heavily on remembering and understanding (55–65% of the skill allocation), so definitions and comparisons matter.

Area I: Information Systems and Data Management

IT Infrastructure

Hardware

- **End-user devices:** workstations, laptops and mobile devices. Thin clients rely on a server for processing.
- **Servers:** file, application, database, web and email servers, and domain controllers that manage network authentication.
- **Network devices:** routers connect networks, switches connect devices within a network, firewalls filter traffic, load balancers spread traffic and wireless access points provide Wi-Fi.
- **Storage:** direct-attached storage, network-attached storage (file level) and storage area networks (block level, high performance).
- **RAID:** RAID 0 stripes data for speed with no redundancy, RAID 1 mirrors, RAID 5 stripes with parity and RAID 10 combines mirroring and striping.

Virtualization runs multiple virtual machines on one physical host through a hypervisor. Type 1 hypervisors run on bare metal, and Type 2 run on a host operating system. **Containers** package an application with its dependencies and

share the host's operating system kernel.

Networks

- **Types:** LAN (one location), WAN (multiple locations), VPN (an encrypted tunnel over a public network) and VLAN (logical segmentation).
- **Architectures:** client-server, peer-to-peer and three-tier (presentation, application and data layers).
- **Protocols:** TCP is reliable and connection-based, UDP is fast without delivery guarantees, IP handles addressing, HTTPS is encrypted web traffic, SFTP is secure file transfer, SMTP sends email, DNS translates names to IP addresses and DHCP assigns IP addresses.

The OSI model, from bottom to top: 1 physical, 2 data link (MAC addresses, switches), 3 network (IP addresses, routers), 4 transport (TCP and UDP), 5 session, 6 presentation (formatting and encryption) and 7 application (HTTP, SMTP).

Cloud Computing

MODEL	THE CUSTOMER MANAGES	THE PROVIDER MANAGES	EXAMPLES
Infrastructure as a service (IaaS)	Operating systems, applications and data	Hardware, storage, networking and virtualization	Virtual servers
Platform as a service (PaaS)	Applications and data	Plus operating systems, middleware and runtime	Application hosting platforms
Software as a service (SaaS)	Data and user access	Nearly everything else	Email, CRM and online accounting software

Deployment models: public (multi-tenant), private (one organization), hybrid (a mix) and community (shared by organizations with common needs).

Essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

The shared responsibility model: the provider secures the cloud infrastructure, and the customer secures what it puts in the cloud, including data, configurations and identities.

Cloud risks: data location and the laws that apply, vendor lock-in, availability commitments, multi-tenant exposure and reliance on the provider's controls. Customers address these through encryption, identity and access management, monitoring, contracts and service level agreements, and **SOC reports** on the provider.

Information Systems and Business Processes

Enterprise resource planning (ERP) systems integrate modules such as finance, procurement, sales, inventory and HR on a common database, which reduces duplicate entry but concentrates risk in access and configuration.

Key business process cycles

- **Order to cash:** customer order, credit approval, shipping, billing and collection
- **Procure to pay:** requisition, purchase order, receiving, invoice matching and payment
- **Record to report:** journal entries, reconciliations and financial statements
- **Hire to retire (payroll):** hiring, timekeeping, payroll processing and termination

Each cycle depends on **segregation of duties**, keeping authorization, recording and custody separate, and on application controls.

Application controls

- **Input:** edit and validation checks, such as field, limit, range, reasonableness, check digit and completeness checks
- **Processing:** control totals, hash totals, record counts, sequence checks and reconciliations
- **Output:** report review, distribution to authorized users and reconciliation to inputs

IT General Controls

ITGCs support the reliable operation of applications:

1. **Access to programs and data:** provisioning, periodic access reviews, prompt removal of access for terminated users, privileged access management and passwords with MFA.
2. **Program changes:** request, approval, testing in a separate environment, segregation between developers and those who move changes to production, version control and post-implementation review. Emergency changes are documented and reviewed afterward.
3. **Program development:** governance of new systems through the system development life cycle.
4. **Computer operations:** job scheduling, monitoring, incident handling, and backup and recovery.

If ITGCs aren't effective, auditors generally can't rely on automated application controls.

SYSTEM DEVELOPMENT

The system development life cycle (SDLC): planning, analysis and requirements, design, development, testing, deployment and maintenance.

- **Testing types:** unit, integration, system, user acceptance, regression, performance and security testing.
- **Methodologies:** waterfall is sequential and structured. Agile, including Scrum, works in short iterations called sprints. DevOps integrates development and operations with continuous integration and delivery.
- **Conversion methods:** parallel (run old and new together, safest), direct cutover (riskiest), phased and pilot.

Business Continuity and Disaster Recovery

A **business impact analysis** identifies critical processes and sets:

- **Maximum tolerable downtime:** the longest outage the business can survive
- **Recovery time objective (RTO):** the target time to restore a system

- **Recovery point objective (RPO):** the maximum acceptable data loss, measured in time

Recovery sites: a **hot site** is fully equipped and ready almost immediately, a **warm site** is partly equipped, and a **cold site** offers only space and utilities. Cloud-based recovery is increasingly common.

Backups

- **Full:** a complete copy. Slowest to make, fastest to restore.
- **Incremental:** changes since the last backup of any type. Fastest to make, slowest to restore.
- **Differential:** changes since the last full backup.
- **The 3-2-1 rule:** three copies, on two types of media, with one offsite.

Plans should be tested regularly, through tabletop exercises, simulations and full failover tests, and updated after changes.

Data Management

DATABASES

Relational databases store data in tables of rows (records) and columns (fields).

- A **primary key** uniquely identifies each record. A **foreign key** links to another table's primary key.
- **Referential integrity** requires every foreign key to match an existing primary key.
- **ACID** properties keep transactions reliable: atomicity (all or nothing), consistency, isolation and durability.
- **Normalization** removes redundancy. First normal form has atomic values with no repeating groups, second removes partial dependencies and third removes transitive dependencies.

Basic SQL

- **SELECT** chooses columns, **FROM** chooses tables and **WHERE** filters rows.
- **JOIN** combines tables on related keys.
- **GROUP BY** aggregates with functions such as SUM, COUNT and AVG. **HAVING** filters the aggregated groups.
- **ORDER BY** sorts results.

Other structures

- **NoSQL databases**, such as document, key-value, column and graph stores, offer flexible schemas and often favor availability and eventual consistency.
- **Data warehouses** hold integrated, historical data optimized for analysis (OLAP), as opposed to transaction processing systems (OLTP).
- **Data lakes** store raw data in its native format, whether structured, semi-structured or unstructured.

ETL (extract, transform, load) moves data from sources into a warehouse.

DATA GOVERNANCE AND THE DATA LIFE CYCLE

- **Roles:** data owners are accountable, data stewards manage quality day to day and data custodians maintain the systems.
- **Data quality:** accuracy, completeness, consistency, timeliness, validity and uniqueness.
- **Metadata and data dictionaries** describe data elements, formats and business rules.
- **Classification:** for example public, internal, confidential and restricted, which drives handling requirements.

The data life cycle: creation or collection, storage, use, sharing, archiving and destruction.

- **Retention schedules** reflect legal, tax and business requirements.
- **Secure disposal** means overwriting, cryptographic erasure or physical destruction, with documentation.

ANALYTICS AND AI

- **Types of analytics:** descriptive, diagnostic, predictive and prescriptive.
- **Machine learning:** supervised learning uses labeled data for classification and regression. Unsupervised learning finds patterns in unlabeled data through clustering and anomaly detection. Reinforcement learning learns by trial and reward.
- **AI risks:** biased training data, lack of explainability, privacy, data leakage and errors such as fabricated outputs. Controls include data governance, model validation, monitoring, human review and access restrictions.

Area II: Security, Confidentiality and Privacy

Security Principles

The CIA triad

- **Confidentiality:** only authorized users can access information, through encryption, access controls and classification.
- **Integrity:** information is accurate and unaltered, through hashing, digital signatures and change controls.
- **Availability:** systems and data are accessible when needed, through redundancy, backups and protection against denial-of-service attacks.

Related concepts are **authentication** (proving identity) and **nonrepudiation** (a sender can't deny an action, as with digital signatures).

Frameworks and Standards

NIST Cybersecurity Framework 2.0 (2024) has six core functions:

1. **Govern:** strategy, policy, roles and supply chain risk oversight, added in version 2.0
2. **Identify:** assets, risks and improvement opportunities

3. **Protect:** safeguards such as access control, training and data security
4. **Detect:** finding cybersecurity events
5. **Respond:** acting on detected incidents
6. **Recover:** restoring operations

Its **implementation tiers** range from Tier 1, partial, to Tier 4, adaptive. **Profiles** describe current and target states.

Other frameworks

- **NIST SP 800-53:** a catalog of security and privacy controls, used widely by federal agencies.
- **ISO/IEC 27001:** the requirements for an information security management system (ISMS), which can be certified. **ISO/IEC 27002** gives guidance on controls. The 2022 version groups 93 controls into four themes: organizational, people, physical and technological.
- **COBIT 2019:** a framework for governance and management of enterprise IT that separates governance from management.
- **CIS Critical Security Controls, version 8:** 18 prioritized controls, implemented in three implementation groups (IG1 to IG3) based on an organization's resources and risk.
- **COSO Internal Control — Integrated Framework (2013):** five components and 17 principles, which apply to IT controls too.

Common Threats

- **Social engineering:** phishing (fraudulent emails), spear phishing (targeted), whaling (aimed at executives), vishing (by phone), smishing (by text) and pretexting.
- **Business email compromise:** impersonating executives or vendors to redirect payments.
- **Malware:** viruses, worms, trojans, spyware and **ransomware**, which encrypts data and demands payment.
- **Denial of service and distributed denial of service:** overwhelming systems to make them unavailable.
- **Man-in-the-middle attacks:** intercepting communications.
- **SQL injection and cross-site scripting:** exploiting weak input validation in applications.
- **Password attacks:** brute force, dictionary attacks and credential stuffing with leaked passwords.
- **Insider threats:** malicious or careless employees and contractors.
- **Advanced persistent threats:** long-term, stealthy intrusions.
- **Supply chain attacks:** compromising vendors or software updates.

Access Controls

Access control models

- **Discretionary (DAC):** the owner decides who has access.
- **Mandatory (MAC):** the system enforces access based on labels and clearances, as in the military.
- **Role-based (RBAC):** permissions are assigned to roles, and users to roles. The most common in business.

- **Attribute-based (ABAC):** access depends on attributes of the user, resource and environment, such as location or time.

Principles: least privilege, need to know, segregation of duties and periodic access reviews.

Authentication factors

- **Something you know:** passwords and PINs
- **Something you have:** tokens, smart cards and authenticator apps
- **Something you are:** fingerprints, facial recognition and other biometrics

Multifactor authentication requires factors from two or more different categories. Two passwords are not MFA.

Passwords: current NIST guidance favors long passphrases, screening against breached-password lists and changing passwords only when compromise is suspected, rather than on a fixed schedule. Systems should store passwords as salted hashes.

Single sign-on uses technologies such as SAML, OAuth and OpenID Connect to give one login across systems. It's convenient, but the central credential becomes a high-value target, so MFA is important.

Privileged access management controls administrator and service accounts through just-in-time access, password vaulting, session recording and monitoring.

Encryption

- **Symmetric encryption** uses one shared key and is fast. AES is the current standard. DES is obsolete. The challenge is distributing the key securely.
- **Asymmetric encryption** uses a public key and a private key, such as RSA and elliptic curve cryptography. It's slower, so it's typically used to exchange symmetric keys and to create digital signatures.
- **Hashing** is a one-way function producing a fixed-length digest, such as SHA-256. It's used for integrity checks and password storage. MD5 and SHA-1 are considered weak.

Digital signatures: the sender hashes the message and encrypts the hash with the sender's **private key**. The recipient decrypts it with the sender's **public key** and compares hashes. This provides authentication, integrity and nonrepudiation.

Public key infrastructure: certificate authorities issue digital certificates (X.509) that bind a public key to an identity. Revoked certificates are checked through revocation lists or online status checks.

Data at rest is protected with full-disk, database and file encryption. **Data in transit** is protected with TLS (HTTPS), VPNs and SSH. **Key management** covers generating, storing (for example in hardware security modules), rotating and destroying keys.

Network Security

- **Firewalls:** packet-filtering, stateful inspection, application-level proxy and next-generation firewalls with deep packet inspection. Rules should deny by default.

- **DMZ:** a separate network segment for public-facing servers.
- **Intrusion detection systems** alert, and **intrusion prevention systems** block. Signature-based detection catches known attacks. Anomaly-based detection can catch new attacks but produces more false positives.
- **Segmentation** with VLANs, subnets and internal firewalls limits how far an attacker can move.
- **Zero trust:** never trust, always verify every request, regardless of network location.
- **Wireless:** use WPA3, or at least WPA2, and enterprise authentication (802.1X). Isolate guest networks. Hiding the network name and filtering by MAC address are weak defenses.
- **Monitoring:** a security information and event management (SIEM) system aggregates and analyzes logs. Vulnerability scanning and penetration testing find weaknesses.

Penetration tests may be black box (no inside knowledge), white box (full knowledge) or gray box (partial). They follow agreed rules of engagement: reconnaissance, scanning, exploitation, post-exploitation and reporting.

Cybersecurity Risk Assessment

1. Identify assets and their value.
2. Identify threats and vulnerabilities.
3. Assess likelihood and impact.
4. Prioritize risks, for example with a heat map.
5. Select responses.

Quantifying risk

- Single loss expectancy (SLE) = asset value × exposure factor
- **Annualized loss expectancy (ALE) = SLE × annualized rate of occurrence (ARO)**
- A control is worth it when the reduction in ALE exceeds its annual cost.

Risk responses: accept, mitigate, transfer (such as through cyber insurance or outsourcing) or avoid.

Types of controls: preventive, detective, corrective, deterrent and compensating. They may be administrative, technical or physical.

Confidentiality and Privacy

Confidentiality protects information designated as confidential, such as trade secrets and business plans. **Privacy** protects personal information about individuals.

KEY PRIVACY LAWS AND STANDARDS

LAW OR STANDARD	SCOPE	HIGHLIGHTS
GDPR (EU)	Personal data of individuals in the EU, wherever processed	Principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and accountability. Rights to access, rectification, erasure, portability and objection. Breach notice to regulators within 72 hours. Fines up to €20 million or 4% of global annual turnover
CCPA, as amended by CPRA (California)	California consumers' personal information held by covered businesses	Rights to know, delete, correct and opt out of the sale or sharing of personal information. Enforced by the California Privacy Protection Agency
HIPAA (U.S. health)	Covered entities and their business associates handling protected health information	Privacy Rule, Security Rule (administrative, physical and technical safeguards) and Breach Notification Rule, with notice to individuals within 60 days
GLBA (U.S. financial)	Financial institutions	Privacy notices and safeguards for customer information
PCI DSS (industry standard)	Anyone storing, processing or transmitting payment card data	12 requirements, including network security controls, protecting stored data, encrypting transmission, access restriction, logging and monitoring, and testing

Privacy practices: privacy by design, data minimization, notice and consent, privacy impact assessments, vendor agreements and anonymization or pseudonymization.

Incident Response

The incident response life cycle

1. **Preparation:** a plan, a trained team, tools and a communication plan
2. **Detection and analysis:** confirm the incident and determine its scope
3. **Containment:** isolate affected systems, first short-term, then long-term
4. **Eradication:** remove the cause and close the vulnerabilities
5. **Recovery:** restore systems and monitor for recurrence
6. **Post-incident activity:** lessons learned and updated defenses

Evidence handling: preserve a **chain of custody**, work on forensic copies, use write-blockers and collect volatile data, such as memory, before it's lost.

Communication: notify management, legal and other stakeholders internally. Notify regulators, law enforcement, affected individuals and business partners as laws and contracts require. Stick to facts.

Area III: SOC Engagements

Overview

A **service organization** provides services to **user entities**, such as payroll processing, cloud hosting or claims processing. A CPA, the **service auditor**, examines the service organization's controls under the AICPA attestation standards (SSAE 18 and later). **User auditors** use SOC 1 reports in their financial statement audits.

REPORT	SUBJECT	INTENDED USERS
SOC 1	Controls relevant to user entities' internal control over financial reporting, against control objectives set by management (AT-C 320)	User entities and their auditors. Restricted use
SOC 2	Controls relevant to the Trust Services Criteria for security, availability, processing integrity, confidentiality or privacy	Customers, regulators, business partners and others with sufficient knowledge. Restricted use
SOC 3	The same Trust Services Criteria, in a short report without detailed tests	General use, such as posting on a website
SOC for Cybersecurity	An entity's cybersecurity risk management program	General use

Type 1 or Type 2

- **Type 1:** as of a specific date. It covers the fairness of the description and the **suitability of design** of controls. The auditor evaluates design and implementation but doesn't test operating effectiveness.
- **Type 2:** over a period of time. It also covers **operating effectiveness**, includes a description of the tests performed and their results, and is far more useful to users. Periods are typically 6 to 12 months. The standards don't set a minimum, but periods shorter than six months are uncommon.

Management's Description and Assertion

The service organization's management provides a **description of the system** and a written **assertion**. The description covers:

- The services provided
- The components of the system: infrastructure, software, people, procedures and data
- The control objectives (SOC 1), or the service commitments and system requirements (SOC 2), and the related controls
- **Complementary user entity controls (CUECs):** controls the user entities must have for the control objectives or criteria to be met, such as reviewing payroll reports and approving time records

- **Subservice organizations** and how they're presented, along with any complementary subservice organization controls
- Significant changes during the period

Subservice organizations

- **Carve-out method:** the subservice organization's controls are excluded from the description and the service auditor's scope. Users may need a separate report on the subservice organization.
- **Inclusive method:** its controls are included, and the service auditor's procedures extend to it.

The Trust Services Criteria (2017, Revised Points of Focus 2022)

1. **Security (the common criteria):** protection against unauthorized access, use or modification. Always included in a SOC 2.
2. **Availability:** the system is available for operation and use as committed.
3. **Processing integrity:** processing is complete, valid, accurate, timely and authorized.
4. **Confidentiality:** information designated as confidential is protected.
5. **Privacy:** personal information is collected, used, retained, disclosed and disposed of in line with the entity's objectives. The privacy criteria replaced the older Generally Accepted Privacy Principles.

The common criteria are organized using the COSO components, plus additional criteria for logical and physical access, system operations, change management and risk mitigation.

Performing the Engagement

1. **Accept the engagement** and agree on its terms: Type 1 or 2, the period and which criteria. Management must provide its description and assertion.
2. **Understand the system** and the service organization's environment, and assess the risks that the description isn't fairly presented or controls aren't suitably designed or operating effectively.
3. **Evaluate the description** against the description criteria.
4. **Evaluate design and implementation** of controls.
5. **Test operating effectiveness** (Type 2) through inquiry combined with observation, inspection and reperformance. Sample sizes depend on how often a control operates and the risk.
 - *Access testing:* select users and confirm access fits their roles and was removed promptly on termination.
 - *Change testing:* select changes and confirm approval, testing and segregation of duties.
6. **Evaluate deviations:** describe them in the tests and results section, and consider their effect on the opinion.
7. **Obtain written representations** from management.
8. **Document the engagement.** Documentation is generally retained for at least five years.

The Service Auditor's Report

An unmodified opinion states that:

- The description fairly presents the system.
- The controls were suitably designed to achieve the control objectives or meet the criteria.
- For Type 2, the controls operated effectively throughout the period.

The opinion is modified, as qualified, adverse or a disclaimer, if the description isn't fairly presented, controls aren't suitably designed, controls didn't operate effectively (Type 2) or the auditor can't obtain sufficient evidence.

How Users Use the Reports

User auditors (SOC 1) check that:

- The report covers the relevant services, controls and period. A **gap period** between the report's end date and the user's year-end may require a bridge letter or other procedures.
- The opinion is unmodified, and any deviations are understood.
- The user entity has the **complementary user entity controls** in place.
- Subservice organizations that were carved out are addressed.

If the controls are effective, the user auditor may reduce substantive testing.

User entities (SOC 2) use the report for vendor risk management. They look for whether the criteria cover their concerns, any exceptions, the CUECs they need and whether the report is current.

Quick Reference

TOPIC	REMEMBER
SOC 1 vs. SOC 2	Financial reporting controls vs. the Trust Services Criteria
Type 1 vs. Type 2	Design at a point in time vs. operating effectiveness over a period
SOC 3	A general-use summary of a SOC 2-type engagement
NIST CSF 2.0	Govern, Identify, Protect, Detect, Respond, Recover
RTO vs. RPO	Time to recover vs. acceptable data loss
Digital signature	Sign with the sender's private key, verify with the sender's public key
ALE	$SLE \times ARO$
Cloud	IaaS, PaaS, SaaS, and the shared responsibility model