CC Certification Study Notes

Code: CC

Security Principles (26%)

Security Principles & Governance

CIA Triad, risk management, controls, governance, and professional ethics

> **Domain Weight**
>
> Security Principles accounts for 26% of the CC exam.

Security Principles is the highest-weighted domain on the ISC² CC exam. Questions test whether you can apply foundational concepts — not just define them — in organizational scenarios involving policies, risk, and control selection.

Confidentiality

Protect information from unauthorized disclosure. Controls: encryption, access controls, data classification, NDAs, need-to-know.

Integrity

Ensure data is accurate and unaltered. Controls: hashing, digital signatures, change management, version control, checksums.

Availability

Ensure systems and data are accessible when needed. Controls: redundancy, backups, DDoS protection, patching, capacity planning.

Risk Management Lifecycle

- Identify assets, threats, and vulnerabilities — inventory what you protect and what can go wrong
- Assess risk: likelihood × impact; qualitative (low/medium/high) vs quantitative (ALE, SLE, ARO)
- Respond: mitigate (controls), transfer (insurance), accept (documented), avoid (stop the activity)
- Monitor continuously — risk is not a one-time exercise

Control Type	Examples	Exam Focus
Administrative	Policies, training, background checks, separation of duties	Often the FIRST control to implement
Technical	Firewalls, encryption, MFA, IDS/IPS	Enforce what policies require
Physical	Locks, badges, CCTV, mantraps, environmental controls	Protect facilities and hardware

> **Governance vs Management**
>
> Governance sets direction and accountability (board, policies, standards). Management implements day-to-day operations. Exam scenarios often ask which body owns policy approval vs operational enforcement.

ISC² Code of Ethics

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

Exam Focus Areas

- Distinguish preventive vs detective vs corrective vs compensating controls
- Know when to recommend policy/training (administrative) vs technical controls
- Risk acceptance requires documented management approval — not ignoring risk

Practice This Domain

Test your understanding with free practice questions at /certifications/isc2/cc/practice — focus on: Confidentiality, Integrity, Availability (CIA Triad), Risk management concepts, Security controls (physical, technical, administrative).

Incident Response, Business Continuity and Disaster Recovery Concepts (10%)

Incident Response & Business Continuity

IR phases, BCP/DRP, RTO/RPO, and backup strategies

Domain Weight

Incident Response, Business Continuity and Disaster Recovery Concepts accounts for 10% of the CC exam.

This domain connects operational security with organizational resilience. Expect scenario questions that ask you to pick the right phase, metric, or recovery strategy.

IR Phase	Key Activities
Preparation	Policies, playbooks, tools, training, communication plans
Detection & Analysis	Alerts, triage, scope determination, evidence preservation
Containment	Isolate affected systems; short-term vs long-term containment
Eradication	Remove malware, close vulnerabilities, patch systems

IR Phase	Key Activities
Recovery	Restore from clean backups; validate before returning to production
Post-Incident	Lessons learned, root cause analysis, update procedures

RTO (Recovery Time Objective)

Maximum acceptable downtime before business impact becomes unacceptable. Drives hot/warm/cold site decisions.

RPO (Recovery Point Objective)

Maximum acceptable data loss measured in time. Drives backup frequency and replication strategy.

BCP vs DRP

- Business Continuity Planning (BCP): keep critical business functions running during disruption
- Disaster Recovery Planning (DRP): restore IT systems and data after a disaster
- BCP is broader (people, facilities, communications); DRP is IT-focused
- Both require testing — tabletop exercises, walkthroughs, simulations, full interruption tests

Backup Strategy

Follow the 3-2-1 rule: 3 copies, 2 different media, 1 offsite. Test restores regularly — backups you cannot restore are not backups.

Exam Focus Areas

- Containment comes before eradication — stop spread first
- Lower RPO requires more frequent backups or synchronous replication
- Post-incident activities include updating IR plans, not just closing tickets

Practice This Domain

Test your understanding with free practice questions at /certifications/isc2/cc/practice — focus on: Incident response phases (preparation, detection, containment, eradication, recovery), Business continuity planning (BCP), Disaster recovery planning (DRP).

Access Controls Concepts (22%)

Access Control Models & Identity

Authentication, authorization, IAM, and least privilege

Domain Weight

Access Controls Concepts accounts for 22% of the CC exam.

Access control questions frequently present a role or data sensitivity scenario and ask which model or practice best fits.

Model	How Access Is Granted	Typical Use
DAC (Discretionary)	Owner decides who gets access	User-owned files, small teams
MAC (Mandatory)	System-enforced labels (classification levels)	Military, government, high classification
RBAC (Role-Based)	Permissions assigned to roles, users get roles	Enterprise IT, least privilege at scale
ABAC (Attribute-Based)	Policies based on attributes (dept, location, time)	Cloud, dynamic environments

Authentication Factors

- Something you know — password, PIN (weakest alone)
- Something you have — smart card, hardware token, authenticator app
- Something you are — fingerprint, facial recognition, biometrics
- Somewhere you are — geolocation, network context
- MFA combines two or more factor types — strongly preferred over password alone

Core IAM Principles

- Least privilege — grant minimum access needed for the job function
- Separation of duties — no single person controls entire critical process
- Need to know — access limited to information required for role
- Provisioning/deprovisioning — timely account lifecycle; remove access on termination
- Periodic access reviews — recertify permissions regularly

> **Common Exam Trap**
>
> MAC is label-based and system-enforced — not the same as "mandatory password changes." DAC lets owners share; RBAC uses job roles.

Exam Focus Areas

- RBAC is the default answer for enterprise role management
- MAC uses security labels (Top Secret, Confidential) — users cannot override
- Separation of duties prevents fraud; least privilege limits blast radius

> **Practice This Domain**
>
> Test your understanding with free practice questions at /certifications/isc2/cc/practice — focus on: Authentication methods (passwords, MFA, biometrics), Authorization and access control models (DAC, MAC, RBAC), Identity management.

Network Security (24%)

Network Security Fundamentals

OSI/TCP-IP, protocols, firewalls, VPNs, and wireless security

> **Domain Weight**
>
> Network Security accounts for 24% of the CC exam.

CC-level network questions focus on how security controls map to network layers and which protocol or device solves a given problem.

Layer	Protocols / Devices	Security Relevance
Layer 2 (Data Link)	MAC addresses, switches, VLANs	ARP spoofing, VLAN hopping, port security
Layer 3 (Network)	IP, routers, ICMP	IP spoofing, routing attacks, ACLs
Layer 4 (Transport)	TCP, UDP	SYN floods, port scanning
Layer 7 (Application)	HTTP/S, DNS, FTP, DHCP	WAF, DNS filtering, application attacks

Network Security Controls

- Firewalls — stateful inspection, application-layer filtering, default deny
- Network segmentation — DMZ, VLANs, micro-segmentation limit lateral movement
- VPN — site-to-site (IPsec) and remote access (SSL/TLS VPN) encrypt traffic
- IDS vs IPS — detect vs actively block; often deployed at network perimeter and internally
- NAC — controls device access based on posture/compliance before network join

Wireless Security Evolution

Standard	Key Improvement
WEP	Deprecated — broken encryption, never use
WPA	TKIP — transitional, also deprecated
WPA2	AES-CCMP — standard for years; still common
WPA3	SAE handshake, stronger encryption, protects open networks better

> **DNS & DHCP Security**
>
> DNS poisoning redirects users to malicious sites; DNSSEC validates responses. DHCP snooping on switches prevents rogue DHCP servers on enterprise LANs.

Exam Focus Areas

- HTTPS encrypts web traffic; HTTP does not — always prefer TLS for sensitive data
- WPA3 is current best practice; WEP/WPA-TKIP are obsolete
- Segmentation limits blast radius after a breach

> **Practice This Domain**
>
> Test your understanding with free practice questions at /certifications/isc2/cc/practice — focus on: OSI model and TCP/IP, Network protocols (HTTP, HTTPS, FTP, DNS, DHCP), Firewalls and network segmentation.

Security Operations (18%)

Security Operations

Data protection, physical security, monitoring, and change management

Domain Weight

Security Operations accounts for 18% of the CC exam.

Security Operations covers day-to-day practices that keep organizations secure: how data is classified and handled, how physical assets are protected, and how changes are controlled.

Data Classification & Handling

- Classify data by sensitivity: Public, Internal, Confidential, Restricted (labels vary by org)
- Handling rules follow classification — encryption, access restrictions, disposal methods
- Data at rest — encrypt disks, databases, backups
- Data in transit — TLS, VPN, secure protocols
- Data in use — memory protection, secure enclaves (advanced)
- Secure disposal — degaussing, shredding, cryptographic erasure

Encryption Concepts

Symmetric

Same key encrypts and decrypts (AES). Fast, used for bulk data. Key distribution is the challenge.

Asymmetric

Public/private key pair (RSA, ECC). Slower, used for key exchange and digital signatures.

Monitoring & Operations

- Centralized logging — aggregate logs from servers, network devices, applications
- SIEM — correlates events, generates alerts, supports incident investigation
- Change management — document, approve, test changes; rollback plans required
- Configuration management — baseline configs, detect unauthorized changes
- Security awareness training — phishing simulations, policy acknowledgment

Physical Security

Badge access, visitor logs, CCTV, server room locks, and environmental controls (HVAC, fire suppression) are exam topics. Social engineering bypasses technical controls — training matters.

Exam Focus Areas

- Hashing verifies integrity; encryption protects confidentiality — different purposes
- SIEM correlates logs across sources — not just storage
- Change management requires approval and testing before production deployment

Practice This Domain

Test your understanding with free practice questions at /certifications/isc2/cc/practice — focus on: Data security and encryption, Data classification and handling, Physical security controls.

Our Products