EVERY EXAM PREP · CHEAT SHEET

ISC2 CC Cheat Sheet 2026

The night-before summary, built like the exam.

— Scored questions	**2h** Time limit	**700 out of 1000 points** Passing score
$199 Exam fee	**ISC2** Governing body	

A dense, last-mile review for the ISC2 CC exam — logistics, domains, vocabulary, and traps to check the night before.

Exam Logistics At-a-Glance

Item	Detail
Format	Multiple choice + advanced item types, Computerized Adaptive Testing (CAT)
Duration	2 hours (120 minutes)
Questions	100–125
Passing score	700 out of 1000
Registration cost	U.S. $199
Testing provider	Pearson VUE (worldwide testing centers)
Experience required	None — open to entry-level candidates
Reschedule fee	U.S. $50
Cancellation fee	U.S. $100
Annual Maintenance Fee (AMF)	U.S. $50/year, with a 90-day grace period from the due date

The Five Domains (Quick List)

- Domain 1: Security Principles — 26%
- Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts — 10%
- Domain 3: Access Controls Concepts — 22%
- Domain 4: Network Security — 24%
- Domain 5: Security Operations — 18%

Domains 1, 3, and 4 together make up over 70% of the exam — prioritize study time there, but don't neglect Domain 2 and Domain 5 since every domain is independently testable.

Key Terms and Concepts to Memorize

Domain 1: Security Principles

- CIA Triad: Confidentiality, Integrity, Availability
- AAA framework: Authentication, Authorization, Accounting
- Non-repudiation, least privilege, separation of duties, defense in depth
- Risk terminology: threat, vulnerability, risk, likelihood, impact, risk appetite vs. risk tolerance

- Governance basics: policies, standards, procedures, guidelines (know the hierarchy and which is mandatory vs. discretionary)
- Legal/ethical concepts: (ISC)² Code of Ethics canons and their priority order

Domain 2: BC, DR & Incident Response

- Business Continuity Plan (BCP) vs. Disaster Recovery Plan (DRP) — BCP keeps the business running, DRP restores IT systems
- RTO (Recovery Time Objective) vs. RPO (Recovery Point Objective) — time to restore vs. acceptable data loss
- Incident response lifecycle: preparation, detection/analysis, containment, eradication, recovery, lessons learned
- Backup types: full, incremental, differential — know restore-speed and storage tradeoffs

Domain 3: Access Controls

- Access control models: DAC, MAC, RBAC, ABAC — know who sets permissions in each
- Physical vs. logical access controls
- Multi-factor authentication (MFA) factor categories: something you know/have/are
- Privileged access management, provisioning/deprovisioning

Domain 4: Network Security

- OSI model layers and common attacks/devices at each layer
- Firewalls, IDS vs. IPS (detect vs. actively block), VPNs, network segmentation
- Common ports/protocols conceptually (HTTP/HTTPS, DNS, secure vs. insecure protocol pairs)
- Wireless security basics, Zero Trust concept

Domain 5: Security Operations

- Data lifecycle and data handling (classification, retention, destruction)
- Logging and monitoring, SIEM concept
- Change management and configuration management basics
- Security awareness training purpose

Common Gotchas and Traps

- Don't confuse IDS (detects and alerts) with IPS (detects and blocks) — a frequent trick on network security items.
- DAC lets the data owner grant access; MAC is enforced by a central authority/system based on classification labels — test-writers love swapping these.
- RTO answers "how fast must we recover," RPO answers "how much data can we lose" — read the question stem carefully for which one is asked.
- CAT exams adapt in real time: once you submit an answer, you cannot go back and review or change previous questions.
- "Best" or "most appropriate" answer questions often have multiple technically-correct options — pick the one most aligned with (ISC)²'s risk-averse, least-privilege philosophy rather than the most technically advanced one.
- Policies are mandatory; guidelines are recommendations — mixing these up is a classic governance-question trap.
- The CC has no work-experience prerequisite, unlike CISSP — don't assume you need professional experience to sit for it.

Night-Before Checklist

1. Confirm Pearson VUE appointment time, testing center address, and required photo ID match exactly.
2. Review the five domain weights once more, focusing extra minutes on Security Principles, Network Security, and Access Controls given their higher exam share.
3. Skim the CIA triad, AAA, DAC/MAC/RBAC/ABAC, IDS vs. IPS, and RTO vs. RPO definitions one final time — these are the highest-frequency trap areas.

4. Get full sleep; CAT format rewards steady focus over 2 hours since there is no backtracking.
5. Arrive early with two forms of valid ID if required, and plan for the reschedule/cancellation fee windows in case of emergencies.
6. Remind yourself: no prior experience is required to pass, so trust your domain review rather than assuming you need field experience to answer correctly.

Official sources

- ISC2 — CC Certification Exam Outline: https://www.isc2.org/certifications/cc/cc-certification-exam-outline
- ISC2 — How to Register, Schedule, Cancel, Pay For Your ISC2 Exam: https://www.isc2.org/exams/schedule-exam
- ISC2 — Certified in Cybersecurity (CC) Certification Overview: https://www.isc2.org/certifications/cc

---