

ISC2 CC Cheat Sheet 2026

The night-before summary, built like the exam.

— 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 — 24%
- Domain 2: Security Governance — 17.3%
- Domain 3: Identity And Access Management (IAM) Concepts — 20%
- Domain 4: Networking and Cloud Security Concepts — 21.3%
- Domain 5: Security Operations and Incident Response — 17.3%

Domains 1, 4, and 3 together make up close to two-thirds of the exam — prioritize study time there, but don't neglect Domain 2 and Domain 5, which are tied for the lowest weight and still independently testable.

Key Terms and Concepts to Memorize

Domain 1: Security Principles

- CIA Triad: Confidentiality, Integrity, Availability
- AAA framework: Authentication, Authorization, Accounting
- Non-repudiation and privacy
- Risk terminology: threat, vulnerability, risk, likelihood, impact, risk appetite vs. risk tolerance

- Controls typing: technical, administrative, physical (physical access controls now live here, not in Domain 3)
- Legal/ethical concepts: (ISC)² Code of Ethics canons and their priority order, plus due care and due diligence

Domain 2: Security Governance

- Governance basics: policies, standards, procedures, guidelines (know the hierarchy and which is mandatory vs. discretionary)
- Security awareness training purpose
- Redundancy and business continuity: 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); backup types (full, incremental, differential) — this is now a redundancy sub-topic here, not its own domain
- Measuring cybersecurity effectiveness: key metrics, Key Risk Indicators (KRI), dashboards and reports

Domain 3: Identity And Access Management (IAM) Concepts

- Access control models: DAC, MAC, RBAC, ABAC — know who sets permissions in each
- Least privilege and separation of duties (SoD)
- Multi-factor authentication (MFA) factor categories: something you know/have/are
- Identity lifecycle management: roles definition, provisioning, review, deprovisioning
- Privileged access management

Domain 4: Networking and Cloud Security Concepts

- OSI model layers and common attacks/devices at each layer
- Firewalls, VPNs, network segmentation, defense in depth, and Zero Trust
- Cloud service models (SaaS/PaaS/IaaS), deployment models, and the shared responsibility model between provider and customer
- Common ports/protocols conceptually (HTTP/HTTPS, DNS, secure vs. insecure protocol pairs)
- Wireless security basics

Domain 5: Security Operations and Incident Response

- Data lifecycle and data handling (classification, retention, destruction), encryption, hashing, and quantum resistant cryptography
- Logging and monitoring, SIEM concept
- Incident response lifecycle: preparation, detection/analysis, containment, eradication, recovery, lessons learned
- Threat intelligence and triage: security event triage, threat actors and motivations, threat frameworks
- Security testing: blue/purple/red teaming, vulnerability scanning, threat modeling, physical penetration testing (phishing, tailgating, impersonation)
- Asset protection: asset lifecycle management, End Of Life (EOL) software and devices, configuration and change management

Common Gotchas and Traps

- Domain 2 changed from Business Continuity/Disaster Recovery to Security Governance — BC, DR, and backups now live inside Governance as a redundancy sub-topic, not their own domain, so don't assume Domain 2 questions are about RTOs and backup types.
- 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, Networking and Cloud Security Concepts, and IAM Concepts given their higher exam share.
3. Skim the CIA triad, AAA, DAC/MAC/RBAC/ABAC, Zero Trust vs. defense in depth, 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 (outline effective September 1, 2026): <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 — ISC2 Annual Maintenance Fees (AMF) Overview: <https://www.isc2.org/policies-procedures/amfs-overview>

Free practice questions for this exam: www.everyexamprep.com/exams/isc2-cc/practice-test