CISSP Cheat Sheet 2026

The night-before summary, built like the exam.

— Questions	**3h** Time limit	**700/1000** Passing score
$749 Exam fee	**ISC2** Governing body	

A condensed reference for the Certified Information Systems Security Professional (CISSP) exam, covering logistics, domains, key concepts, and last-minute review points.

Exam Logistics At-a-Glance

Item	Detail
Format	Computerized Adaptive Testing (CAT), English exam
Question count	100 to 150 questions
Passing score	700 out of 1000 points
Registration fee	U.S. $749 (standard)
Rescheduling fee	U.S. $50
Cancellation fee	U.S. $100
Delivery	Pearson VUE test centers
Domains covered	8 domains

Eligibility Requirements

- A minimum of 5 years cumulative, full-time paid work experience is required.
- That experience must span two or more of the eight domains in the current CISSP Exam Outline.
- A relevant degree or approved credential can satisfy 1 year of the required experience.
- Without full experience, candidates can become an Associate of ISC2 and have 6 years to earn the five years required.
- Registration and appointment scheduling happen through the Pearson VUE website after signing up with ISC2.

The 8 Official Domains (Quick List)

1. Security and Risk Management — 16%
2. Asset Security — 10%
3. Security Architecture and Engineering — 13%
4. Communication and Network Security — 13%
5. Identity and Access Management (IAM) — 13%
6. Security Assessment and Testing — 12%
7. Security Operations — 13%
8. Software Development Security — 10%

Notice the weighting: Domain 1 (Security and Risk Management) carries the heaviest single share, and four domains tie at

13% each — Architecture, Network Security, IAM, and Operations. Under-studying Domain 1 is one of the most common scoring mistakes.

Key Terms and Concepts to Memorize

- CIA Triad — Confidentiality, Integrity, Availability; the foundational model behind nearly every domain.
- Due care vs. due diligence — due care is taking reasonable action; due diligence is the research/investigation behind that action.
- Defense in depth — layered, overlapping controls rather than reliance on a single safeguard.
- Least privilege vs. need-to-know — least privilege limits access rights; need-to-know limits access to specific data required for a task.
- Administrative, technical (logical), and physical controls — the three control categories tested across risk and operations questions.
- Qualitative vs. quantitative risk analysis — quantitative uses numeric values (e.g., ALE, SLE, ARO); qualitative uses relative ratings.
- Symmetric vs. asymmetric cryptography — shared-key speed versus public/private-key key-exchange and non-repudiation.
- Authentication factors — something you know, have, and are; multi-factor combines at least two categories.
- Business Continuity Planning (BCP) vs. Disaster Recovery Planning (DRP) — BCP keeps the business running; DRP restores IT systems after disruption.
- Change management vs. configuration management — controlling what changes versus tracking system state and baselines.

Common Gotchas and Traps

- CISSP is a management/governance-oriented exam, not a hands-on technical exam — when two answers seem technically correct, pick the one reflecting policy, process, or risk-based thinking.
- Computerized Adaptive Testing means question difficulty adjusts based on your answers, and you cannot skip back to review or change earlier answers.
- "Best" or "most appropriate" answer questions often have multiple technically valid options — always default to the answer that best protects the organization's risk posture.
- Don't confuse the domain names with their weightings; several domains sound similar (Security Architecture vs. Security Operations) but test very different content.
- Experience requirements must map to the current Exam Outline domains — unrelated IT experience alone does not qualify.
- Missing the Pearson VUE cancellation or rescheduling window triggers a fee, so lock in a realistic test date rather than scheduling too early.

Night-Before Checklist

- Confirm Pearson VUE appointment time, test center address, and required photo ID.
- Review the 8 domain weightings once more, focusing extra attention on Domain 1 given its 16% share.
- Skim key term flashcards: CIA triad, due care/diligence, control types, risk formulas, authentication factors.
- Get full sleep — CAT exams reward careful reading and focus, not last-minute cramming.
- Pack ID, confirmation details, and arrive early to avoid day-of stress.
- Do a final mental review of test-taking strategy: choose the most risk-averse, management-aligned answer when in doubt.

Official sources

- ISC2 — CISSP Certification Exam Outline: https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline
- U.S. Bureau of Labor Statistics — Occupational Employment and Wage Statistics, May 2025 — Information Security

Analysts (SOC 15-1212): https://www.bls.gov/oes/current/oes151212.htm

- ISC2 — CISSP Experience Requirements: https://www.isc2.org/certifications/cissp/cissp-experience-requirements

---

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