

CISM Cheat Sheet 2026

The night-before summary, built like the exam.

150 Scored questions	4h Time limit	450 on a scale of 200 to ... Passing score
\$760 Exam fee	ISACA Governing body	

Certified Information Security Manager (CISM) is ISACA's management-track credential for professionals who oversee an enterprise information security program rather than perform hands-on technical security work. This sheet condenses the logistics, domains, vocabulary, and traps to review the night before your test.

Exam Logistics At a Glance

Item	Detail
Question count	150 multiple-choice questions
Duration	240 minutes (4 hours)
Answer format	4 options per question, one best answer
Passing score	450+ on a scaled 200-800 scale
Member fee	US\$575.00
Non-member fee	US\$760.00
Delivery	In-person test center or online remote proctored via PSI
Reschedule window	48 hours minimum before your appointment
Certification window	5 years from passing to complete the application

Registration Flow

- Register and pay first; ISACA emails you eligibility to schedule with PSI afterward — you cannot book a seat before that confirmation arrives.
- Build in buffer time between registering and your target test date so the eligibility email and PSI scheduling don't rush your prep.
- Cancelling or rescheduling inside the 48-hour window risks forfeiting the fee, so lock your date deliberately.

The Four Job Practice Domains

1. Information Security Governance — 17% of the exam
2. Information Security Risk Management — 20% of the exam
3. Information Security Program — 33% of the exam (the largest domain)
4. Incident Management — 30% of the exam

Domain 3 and Domain 4 together make up nearly two-thirds of the scored questions, so program-building and incident-response content deserves the most review time relative to governance and risk theory.

Key Terms and Concepts to Memorize

- Scaled score, not raw or percentage: your reported score (200-800) is not the count of questions answered correctly, so don't try to reverse-engineer a percentage from it.
- Governance vs. management: governance sets direction, risk appetite, and accountability at the board/executive level; management executes the program day to day — CISM questions frequently test which layer a scenario belongs to.
- Risk appetite vs. risk tolerance: appetite is the broad amount of risk an organization is willing to accept; tolerance is the acceptable variation around a specific risk target.
- Business Impact Analysis (BIA): identifies critical processes and quantifies impact of disruption — feeds recovery time objective (RTO) and recovery point objective (RPO) decisions.
- Incident response lifecycle: preparation, identification, containment, eradication, recovery, and lessons learned — know the order and what belongs in each phase.
- Metrics and KPIs/KRIs: security governance leans heavily on measurable outcomes tied to business objectives, not just technical controls.
- Senior management as the answer: when a CISM question asks who should approve, own, or be accountable for a security decision, the most correct answer is usually escalation to senior management or the steering committee, not a technical fix.

Common Gotchas and Traps

- CISM is a management exam — technical answers that sound rigorous are frequently wrong if a governance, policy, or risk-based answer is also offered.
- Best-answer questions often have two plausible options; pick the one addressing root cause or long-term risk reduction over a quick tactical fix.
- Don't assume you need to memorize product names or specific technologies — CISM tests process, judgment, and organizational alignment, not tools.
- Time management matters: 240 minutes for 150 questions is under 2 minutes per question on average, so flag and move on rather than stalling on any single item.
- Watch for scenario questions that test whether you'd notify legal, regulators, or the incident response team first — sequencing errors are a common trap.
- Remember the exam window logistics are not the same as content mastery — many candidates lose points to careless misreads of least vs. most or first vs. best in the question stem.

Night-Before Checklist

- Confirm your exam mode (test center address or online remote-proctor system requirements) and double-check you are not inside the 48-hour reschedule cutoff.
- Verify accepted identification documents match what your delivery mode requires.
- Do a final pass on domain weightings — spend your last review minutes on Information Security Program and Incident Management, since together they cover the majority of scored questions.
- Skim key term pairs (governance vs. management, appetite vs. tolerance, containment vs. eradication) rather than cramming new material.
- Plan your test-day timing: block out roughly 4 hours, plus travel or system setup time if testing online.
- Get sleep — CISM's scenario-based judgment questions reward clear thinking over last-minute memorization.
- Remember passing requires a scaled score of 450+; a rough sense of your practice-test percentage does not map linearly to this scale, so don't over-index on raw percentage during review.

Official sources

- ISACA — ISACA Certification Exam Candidate Guide:
<https://www.isaca.org/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx>
- ISACA — CISM Exam Content Outline: <https://www.isaca.org/credentialing/cism/cism-exam-content-outline>

- ISACA — CISM Certification Overview: <https://www.isaca.org/credentialing/cism>

Free practice questions for this exam: www.everyexamprep.com/practice/exams/technology/isaca-cism