

ISACA

CISM — Certified Information Security Manager Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

EXPERT

40 HOURS

5 DAYS

At a glance

COURSE	CISM — Certified Information Security Manager
TRACK	ISACA
DOMAIN	Cyber Security
LEVEL	Expert
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a expert course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Four domains, mapped one-for-one to the ISACA CISM exam content outline and taught in the same order, so nothing on the exam is left uncovered.

Each domain below carries the weighting ISACA publishes for it. Two of the four account for just under two thirds of the exam — Information Security Program at 33% and Incident Management at 30% — and the course gives them time in that proportion rather than treating all four as equal.

ISACA has announced a refreshed CISM exam content outline effective 3 November 2026. We teach against the outline that applies to your exam date and confirm which one that is when you book, so check your date against the change before you register.

CISM is a management certification. Almost every question is a judgement call made by someone accountable for a programme and a budget, not by someone at a console. The teaching is built around that distinction, because it is the single most common reason experienced technical candidates fail.

Domain 01 – Information Security Governance

Establishing the authority, structure and strategy that a security programme runs on. 17% of the exam.

- Organisational culture, and how it limits what a security function can realistically enforce
- Legal, regulatory and contractual requirements that bear on the programme
- Organisational structures, roles and responsibilities, including the board and executive relationship
- Developing an information security strategy that follows business objectives rather than threat headlines
- Information governance frameworks and standards, and choosing between them on evidence
- Strategic planning: budgets, resourcing and building a business case that survives scrutiny
- Translating governance intent into policy the programme can be measured against

Domain 02 – Information Security Risk Management

Identifying risk, deciding what to do about it, and making sure someone owns that decision. 20% of the exam.

- The emerging risk and threat landscape, and keeping a risk register that reflects it
- Vulnerability and control deficiency analysis
- Risk assessment and analysis methods, qualitative and quantitative, and where each is credible
- Legal, regulatory, third-party and supply chain risk
- Risk treatment options — mitigate, transfer, avoid, accept — and who is entitled to choose
- Risk and control ownership, and making ownership stick after the meeting ends
- Risk monitoring and reporting, including communicating risk to people without a security background
- Expressing risk in business impact rather than technical severity

Domain 03 – Information Security Program

The largest domain: building the programme, then running it. 33% of the exam.

- Programme resources — people, tooling, technology and the budget to sustain them
- Information asset identification and classification
- Industry standards and frameworks, and the policies, procedures and guidelines built on them
- Information security programme metrics that give management something they can act on

- Control design and selection against identified risk
- Control implementation and integration with business processes and existing technology
- Control testing and evaluation, and evidencing effectiveness to an auditor
- Security awareness and training targeted by role rather than delivered uniformly
- Managing external services: providers, suppliers, third parties and fourth-party exposure
- Programme communication and reporting, from operational detail to board summary

Domain 04 – Incident Management

Preparing for the incident, and then managing it. 30% of the exam.

- Building an incident response plan, and the team and authority that run it
- Business impact analysis, and what it tells you about recovery priorities
- Business continuity and disaster recovery planning, and the recovery objectives that drive both
- Incident classification and categorisation, and the escalation thresholds that follow
- Incident management training, testing and tabletop evaluation
- Incident management tools and techniques
- Incident investigation and evaluation, including evidence handling that survives later scrutiny
- Containment methods, and the trade-off against keeping the business running
- Response communications: internal reporting, customer notification, regulatory disclosure, escalation
- Eradication, recovery, and a post-incident review that actually changes something

Who should take this

Information security managers, heads of security, aspiring CISOs, risk and compliance leads, IT managers moving into security leadership, and consultants who advise at programme level.

ISACA requires five or more years of information security work experience, gained across at least three of the four CISM domains, and within the ten years preceding your application for certification. You may sit the exam before you have it: candidates have five years from the date they pass to apply for certification.

You will need enough technical grounding to follow a control discussion. You do not need to be hands-on, and depth in one technical specialism is not a substitute for breadth across the four domains.

The exam

The CISM is set and awarded by ISACA. It is a fixed-form exam, not adaptive — every candidate answers the same number of questions.

- 150 multiple-choice questions
- Four hours, 240 minutes
- A scaled score of 450 or higher is required to pass
- Available in English, Spanish, Chinese Simplified, Japanese, French and German
- Computer-based, at PSI test centres worldwide or remotely proctored

The exam registration is purchased separately from ISACA. We arrange it on your behalf and send you the details, and you book your own exam date. Passing the exam is one step: certification also requires the experience application to be submitted and verified.

How we deliver it

Four days, classroom or online live, or at your office for a private group. The format is discussion-led — short teaching blocks, then case work where the group has to make a decision as a management team and justify it. Domain checkpoints each day, and a full-length timed mock on the final afternoon with a review of why the wrong answers looked right.

Mapped to the ISACA CISM exam content outline. Taught from Hacky Security's own curriculum by instructors who hold the certification and run security programmes rather than only teach them.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/cism/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.