

ISACA

CRISC — Certified in Risk and Information Systems Control 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.

INTERMEDIATE

40 HOURS

5 DAYS

At a glance

COURSE	CRISC — Certified in Risk and Information Systems Control
TRACK	ISACA
DOMAIN	Cyber Security
LEVEL	Intermediate
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 an intermediate 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 ISACA's CRISC exam content outline and taught in the same order, so nothing on the exam is left uncovered.

The outline that defines the current CRISC took effect for exams on 3 November 2025, following ISACA's job practice review; ISACA released the matching preparation materials on 3 September 2025. The four domain names did not move. The weighting did: Risk Assessment rose to 22% and Technology and Security fell to 20%, with Governance and Risk Response and Reporting unchanged. No further revision has been announced. Each domain below carries its published weighting, and we give it classroom time in proportion.

CRISC is not a controls exam with a risk vocabulary. It asks who owns a risk, whether the response is proportionate to appetite, and what you would report to whom. The teaching is built around that — scenario work on a live risk register rather than definition drills.

Domain 01 — Governance

The frame every later judgement is made inside: what the organisation is trying to do, and how much risk it has agreed to carry doing it. 26% of the exam.

- Strategy, goals and objectives, and tracing an IT risk back to the business outcome it threatens
- Organisational structure, roles and responsibilities, and where risk decisions legitimately sit
- Organisational culture and ethics, and the behaviours that quietly defeat a control
- Policies and standards: writing them so they are enforceable, and reviewing them when they are not
- Business processes and resilience, including business continuity and disaster recovery planning
- Organisational asset management, and knowing what is in scope before you assess anything
- Enterprise risk management and the relationship between IT risk and the enterprise risk picture
- The three lines of defence, and what each line may and may not assure
- Risk profile, risk appetite and risk tolerance, and the difference between them in practice
- Risk frameworks, and legal, regulatory and contractual obligations as inputs to the framework

Domain 02 — Risk Assessment

Identifying what could go wrong, then working out how likely it is and what it would cost. 22% of the exam.

- Risk events, and describing one precisely enough to be assessed rather than argued about
- Threat modelling and reading the current threat landscape against your own estate
- Vulnerability management as an input to risk rather than a metric in its own right
- Risk scenario development and evaluation, and testing a scenario for plausibility
- Risk assessment concepts and the standards that govern them
- Business impact analysis, recovery objectives, and the dependencies people forget to declare
- The risk register: what belongs in it, who maintains it, and how it stays current
- Quantitative and qualitative risk analysis methodologies, and choosing between them honestly
- Inherent risk against residual risk, and the control assumptions that separate the two

Domain 03 – Risk Response and Reporting

The largest domain: deciding what to do, building the control, and telling the right people the truth about it. 32% of the exam.

- Risk response options — accept, mitigate, transfer, avoid — and justifying the one chosen
- Risk ownership and control ownership, and why they are not always the same person
- Vendor and supply chain risk management across the third-party lifecycle
- Managing issues, findings, exceptions and exemptions so they close rather than accumulate
- Control frameworks, control types and standards, and control design, selection and implementation against the risk in question
- Control testing methodologies, and evidence that would survive an auditor
- Risk action plans: ownership, deadlines and tracking to completion
- Data collection, aggregation, analysis and validation underneath any risk number you publish, and the risk and control metrics built on it — key risk, key control and key performance indicators
- Monitoring and reporting techniques, including heat maps, scorecards and dashboards
- Identifying and reporting emerging risks before they become findings

Domain 04 – Technology and Security

Enough technology and security depth to challenge an engineer's assessment rather than accept it. 20% of the exam.

- Technology principles, technology roadmaps and enterprise architecture, and the risk that follows from architectural choice
- Operations management: change management, asset management, DevOps, problem and incident handling
- The system development lifecycle, and where risk is introduced and where it can be caught
- Data lifecycle management from creation through retention to disposal
- Portfolio and project management, including agile delivery and the assurance it changes
- Technology resilience, disaster response and recovery, and testing before you need it
- Emerging technologies, including artificial intelligence, and assessing risk without precedent
- Security concepts, frameworks and standards, and mapping them onto the risk register
- Security and risk awareness and training, and measuring whether behaviour changed
- Data privacy and data protection principles as they bear on risk decisions

Who should take this

IT risk practitioners, risk and control analysts, internal auditors moving into risk, compliance leads, business continuity managers, and security professionals who are being asked to justify controls in business terms rather than technical ones. It also suits project and operations managers who own risk in practice and want the discipline behind it.

ISACA requires three or more years of cumulative work experience in IT risk management and information systems control, across at least two of the four CRISC domains, gained within the ten years before the certification application. There are no experience waivers or substitutions. You can sit the exam before you have the experience: candidates have five years from the date they pass to submit the certification application.

You will need working familiarity with how IT is governed and delivered in an organisation. You do not need to be technically hands-on.

The exam

The CRISC is set and awarded by ISACA. It is computer-based, delivered at authorised PSI testing centres worldwide or by remote proctoring.

- 150 multiple-choice questions
- Four hours, 240 minutes
- A scaled score of 450 or higher is required to pass, on a scale of 200 to 800
- Available in English, Spanish and Japanese

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. Certification also requires an application, an application processing fee, adherence to ISACA's Code of Professional Ethics, and continuing professional education to maintain.

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 assess a scenario, choose a response and defend it to a sceptical stakeholder. Domain checkpoints each day, and a full-length timed mock on the final afternoon.

Mapped to the ISACA CRISC exam content outline effective 3 November 2025. Taught from Hacky Security's own curriculum by instructors who hold the certification and run risk programmes for a living.

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/crisc/>

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 12 September 2026.