

ISACA

CISA — Certified Information Systems Auditor 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	CISA — Certified Information Systems Auditor
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

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

The outline that defines the current CISA took effect on 1 August 2024. The five domain names and their weightings carried over from the previous job practice, but the content inside them was rewritten around disruptive technology and the way IT audit work is actually being done now — cloud-hosted estates, automation, data analytics used as evidence, and resilience as a board-level question. Each domain below carries its published weighting, and we give it classroom time in proportion.

CISA is an assurance exam, not a technology exam. The questions rarely ask how a control works; they ask whether it is operating, what evidence would prove it, and what the auditor should do about what the evidence shows. The teaching is built around that — scenario work, evidence judgement, and practice at picking the best answer when three answers are defensible.

Domain 01 — Information Systems Auditing Process

How an audit is planned, executed and reported, and the standards an IS auditor is held to while doing it. 18% of the exam.

- IS audit standards, guidelines and codes of ethics, and where professional obligation overrides client preference
- Business processes, types of controls, and how control objectives are derived from them
- Risk-based audit planning: scoping, materiality, and deciding where fieldwork time is worth spending
- Audit project management, resourcing, and keeping an engagement inside its terms of reference
- Sampling methodology and testing techniques, and the difference between design effectiveness and operating effectiveness
- Evidence collection: what qualifies, how it is retained, and what makes a finding defensible afterwards
- Data analytics as an audit technique, including testing a full population rather than a sample
- Reporting and communication, from the raised exception through to the agreed management response
- Quality assurance, engagement review, and follow-up on prior-year findings

Domain 02 — Governance and Management of IT

Whether the IT function is being directed and controlled in the interests of the enterprise, and whether anyone can demonstrate it. 18% of the exam.

- IT governance and IT strategy, and how technology direction is tied back to business objectives
- Laws, regulations and industry standards affecting the organisation, and mapping each obligation to an owner
- Organisational structure, roles and responsibilities, and segregation of duties at management level
- Enterprise architecture, and the control implications of the target state being built towards
- Enterprise risk management, risk appetite, and the risk register as an auditable artefact
- Policies, standards, procedures and guidelines: their hierarchy, and evidence that they are actually applied
- Privacy programme and data governance, including data ownership and classification
- IT resource management, budgeting, and capability measured against demand
- Vendor and third-party management: selection, contracts, service levels and ongoing oversight
- Performance monitoring, key indicators, maturity models and management reporting

Domain 03 – Information Systems Acquisition, Development and Implementation

Auditing a system while it is still being built, when a control gap is still cheap to close. 12% of the exam.

- Project governance structures, and the auditor's role at each stage of a programme
- Business case, feasibility study, and benefits realisation tracked beyond go-live
- Development methodologies — waterfall, iterative, agile, DevOps — and what assurance looks like in each
- Control identification and design, including application controls and the audit trail
- Testing methodologies: unit, integration and user acceptance testing, and evidence of sign-off
- Configuration, release and change management across the development pipeline
- System readiness, implementation planning, and the criteria behind a go-live decision
- Data conversion and migration, and proving completeness and accuracy after the move
- Post-implementation review, and whether the benefits claimed were the benefits delivered

Domain 04 – Information Systems Operations and Business Resilience

The joint-largest domain: running systems day to day, and surviving the day they stop. 26% of the exam.

- Common technology components, system interfaces, end-user computing, and the IT asset inventory every other control depends on
- Job scheduling, production automation, and controls around unattended processing
- Shadow IT, and the exposure created by systems nobody has inventoried
- Availability, capacity and performance management, and the distinction between fixing an incident and resolving a problem
- Change, configuration, release and patch management as auditable processes
- IT service level management and outsourcing, and the controls that must follow work out of house
- Database management, integrity controls, and administrator access
- Business impact analysis, recovery objectives, and designing systems to degrade rather than fail
- Data backup, storage and restoration — including proof that restores have been tested, not just scheduled
- Business continuity and disaster recovery plans, exercising them, and auditing what the exercise revealed

Domain 05 – Protection of Information Assets

The security domain, examined from the auditor's chair rather than the engineer's. 26% of the exam.

- Information asset security frameworks, standards and control catalogues
- Physical and environmental controls, and access to facilities and equipment
- Identity and access management: provisioning, privileged access, periodic review and revocation
- Network and endpoint security controls, segmentation and secure configuration
- Data classification, data loss prevention, and handling requirements across the data lifecycle
- Cryptography, public key infrastructure and key management, audited for correct use rather than algorithm choice
- Cloud, virtualisation and mobile computing, and where the shared responsibility boundary actually sits
- Security awareness training, and evidence that it changed behaviour rather than attendance
- Attack methods and techniques, and the security testing, monitoring and log management controls that answer them
- Security incident response, evidence handling and forensics at the level an auditor must understand

Who should take this

IT auditors and internal auditors moving into systems work, IT risk and compliance professionals, security managers who are audited often enough that they would rather understand the process, and finance or external auditors whose scope now includes IT general controls.

ISACA requires five years of professional information systems auditing, control or security work experience, gained within the ten years before the certification application, before it will award CISA. Waivers can reduce that by up to three years — a year of general audit or general information systems work, or a relevant degree, among others — but at least two years cannot be waived. You may sit the exam before you have the experience, and you then have five years from your pass date to apply for certification.

You will need general familiarity with how IT is organised and operated. You do not need to be technical, and you do not need to be able to configure anything.

The exam

The CISA is set and awarded by ISACA, and delivered at a test centre or by remote proctor.

- 150 multiple-choice questions, four hours
- Each question has a stem and four options; some questions are grouped under a shared scenario
- Scores are reported on a scale from 200 to 800, and 450 is the pass mark
- Available in Chinese Simplified, English, French, German, Japanese, Korean and Spanish

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 a separate application evidencing the experience requirement, and agreement to ISACA's code of professional ethics and continuing education policy.

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 audit scenarios where the group has to decide what to test, what evidence would satisfy them, and what they would put in writing. Domain checkpoints each day, and a full-length timed mock on the final afternoon, reviewed for why the wrong answers were attractive.

Mapped to the ISACA CISA exam content outline effective 1 August 2024. Taught from Hacky Security's own curriculum by instructors who hold the certification and run audit and assurance engagements 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/cisa/>

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.