

ISC2

CISSP — Certified Information Systems Security Professional 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.

PROFESSIONAL

40 HOURS

5 DAYS

At a glance

COURSE	CISSP — Certified Information Systems Security Professional
TRACK	ISC2
DOMAIN	Cyber Security
LEVEL	Professional
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 professional 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

Eight domains, mapped one-for-one to the ISC2 CISSP exam outline and taught in the same order, so nothing on the exam is left uncovered.

The outline that defines the current CISSP took effect on 15 April 2024, following ISC2's job task analysis. The domain names did not move, but the weighting did, and the content inside several domains was rewritten around cloud-native architecture, zero trust, supply chain risk and the software toolchain. Each domain below carries its published weighting, and we give it classroom time in proportion.

CISSP is a management exam wearing a technical vocabulary. The questions rarely ask what a control does; they ask which control you would choose, in whose interest, and what you would give up to get it. The teaching is built around that — scenario discussion and decision practice rather than memorising lists.

Domain 01 – Security and Risk Management

The largest domain, and the one that sets the frame every other domain is judged inside. 16% of the exam.

- Professional ethics: the ISC2 Code of Professional Ethics and organisational codes of conduct
- Core security concepts — confidentiality, integrity, availability, authenticity and non-repudiation — and the governance principles that align them to business strategy, including due care against due diligence
- Legal, regulatory and compliance obligations across jurisdictions: privacy, contracts, cybercrime
- Investigation types — administrative, criminal, civil, regulatory, industry — and the evidence standard each one demands
- Policy, standards, procedures and guidelines: writing them, and making them hold
- Business continuity requirements, business impact analysis and recovery prioritisation
- Personnel security across the employment lifecycle, from screening to termination
- Risk management concepts: identification, assessment, treatment, monitoring and reporting, and supply chain risk across products, suppliers and service providers
- Threat modelling methodologies, and using their output to choose controls
- Security awareness, education and training, and measuring whether any of it worked

Domain 02 – Asset Security

What you hold, who owns it, and what happens to it at every stage of its life. 10% of the exam.

- Identifying and classifying information and assets by sensitivity and business value
- Ownership roles: data owner, custodian, processor, controller, and who is accountable
- Handling requirements, labelling and marking as an asset moves between systems and people
- Secure provisioning, asset inventory and configuration baselines
- The data lifecycle: collection, location, maintenance, retention and destruction
- Retention decisions, end of life and end of support, and secure disposal
- Data states, and the controls that suit data at rest, in transit and in use
- Data loss prevention, tokenisation, anonymisation, and scoping and tailoring of baselines

Domain 03 — Security Architecture and Engineering

Designing a system that is secure by construction rather than by later correction. 13% of the exam.

- Secure design principles: least privilege, defence in depth, zero trust, secure defaults, fail securely
- Security models and what each one actually enforces — Bell-LaPadula, Biba, Clark-Wilson, the Star Model
- Selecting controls against system security requirements and recognised evaluation criteria
- Security capabilities of information systems: memory protection, Trusted Platform Module, encryption and decryption
- Architectural vulnerabilities across client-server, database, industrial control, embedded, virtualised, containerised, serverless and high-performance systems
- Selecting cryptographic solutions: symmetric and asymmetric algorithms, elliptic curve, hashing, digital signatures, Public Key Infrastructure and key management
- Cryptanalytic attack methods, from brute force and side channel to the way ransomware weaponises good cryptography
- Applying security principles to site and facility design, and the physical controls that follow
- Managing the information system lifecycle from requirements through to decommissioning

Domain 04 — Communication and Network Security

Network design as a security decision, not a connectivity decision. 13% of the exam.

- The OSI and TCP/IP models, and where a control belongs at each layer
- IPv4 and IPv6 addressing, and secure protocols including IPsec, TLS and DNSSEC
- Segmentation, micro-segmentation, zero trust network access and software-defined networking
- Wireless, cellular and satellite networks and the exposure particular to each
- Content distribution networks, edge computing and virtual private cloud networking
- Securing network components: transmission media, network access control, endpoint security
- Secure communication channels for voice, collaboration, remote access and third-party connectivity
- Multilayer and converged protocols, and the risk that encapsulation hides

Domain 05 — Identity and Access Management (IAM)

Who gets in, what they can reach once inside, and how that is taken back. 13% of the exam.

- Controlling physical and logical access to information, systems, devices and facilities
- Designing an identification and authentication strategy for people, devices and services
- Authentication factors, multifactor authentication and passwordless approaches
- Federated identity with third-party services, and the protocols that carry it
- Authorisation mechanisms: role-based, rule-based, attribute-based, mandatory and discretionary access control
- The identity and access provisioning lifecycle — registration, review, revocation
- Single sign-on, just-in-time access and privileged access management
- Credential management systems, directory services, and how accounts get compromised

Domain 06 — Security Assessment and Testing

Finding out whether the controls you designed are the controls you have. 12% of the exam.

- Designing assessment, test and audit strategies for internal, external and third-party scope

- Vulnerability assessment and penetration testing run as a control rather than an event
- Log review, synthetic transactions, and code review and testing
- Misuse case testing, test coverage analysis and interface testing
- Breach and attack simulation, and compliance checks
- Collecting security process data: account management, backup verification, training, disaster recovery
- Analysing test output and writing a report that produces remediation rather than filing
- Conducting and facilitating internal, external and third-party audits

Domain 07 — Security Operations

The day-to-day discipline that decides whether the rest of the programme survives contact with reality. 13% of the exam.

- Investigations: evidence collection and handling, digital forensics, chain of custody, reporting
- Logging and monitoring — SIEM, continuous monitoring, egress monitoring, threat intelligence and threat hunting
- Configuration management: provisioning, baselining and automation
- Foundational operations concepts: need to know, least privilege, separation of duties, job rotation
- Resource protection for media, hardware and software assets
- Incident management from detection through response, mitigation, reporting, recovery and lessons learned
- Detective and preventative measures: firewalls, intrusion detection and prevention, allow-listing, sandboxing, honeypots, anti-malware
- Patch and vulnerability management, and participating in change management
- Recovery strategies, disaster recovery processes, and testing the plan before you need it
- Physical security, personnel safety and duress, including travel and remote working

Domain 08 — Software Development Security

Security applied where the defects are actually introduced. 10% of the exam.

- Integrating security across the software development lifecycle, from waterfall to agile and DevSecOps
- Development methodologies, maturity models, operation and maintenance, and change management
- Security controls in development ecosystems: toolchains, repositories, CI/CD pipelines and integrated development environments
- Programming language weaknesses, library and runtime risk, and application security testing
- Assessing the effectiveness of software security through auditing, logging and risk analysis
- Assessing acquired software: commercial products, open source, managed services and cloud services
- Software composition analysis and the software bill of materials
- Secure coding guidelines and standards, and the defect classes they exist to prevent

Who should take this

Security managers, security architects, consultants, risk and compliance leads, and senior engineers who are being asked to own decisions rather than implement them. It also suits experienced practitioners who have depth in two or three domains and need the other five before they can operate at programme level.

ISC2 requires five years of cumulative paid work experience across two or more of the eight domains before it will award the certification. A relevant degree or an approved credential can satisfy one of those years. Candidates who do not yet have the experience can sit the exam and become an Associate of ISC2 while they accrue it.

You will need broad working knowledge across security, networking and systems. You do not need to be currently hands-on.

The exam

The CISSP is set and awarded by ISC2, and is delivered worldwide using Computerized Adaptive Testing. The questions you see depend on how you answered the ones before, so there is no fixed paper and no benefit in pacing against a question count.

- 100 to 150 items, three hours
- Adaptive format, with multiple choice and advanced item types
- A scaled score of 700 out of 1000 is required to pass
- Available in Chinese, English, German, Japanese and Spanish

The exam voucher is purchased separately from ISC2. We arrange it on your behalf and send you the code, and you book your own exam date. Certification also requires endorsement by an existing ISC2 member once you pass.

How we deliver it

Five days, classroom or online live, or at your office for a private group. The format is discussion-led: short teaching blocks, then scenario work where the group has to defend a decision. Domain checkpoints each day, and a full-length adaptive mock under exam conditions on the final afternoon.

Mapped to the ISC2 CISSP exam outline effective 15 April 2024. Taught from Hacky Security's own curriculum by instructors who hold the certification and run security 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/cissp/>

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.