

CISSP — Certified Information Systems Security Professional

Course Duration ~50 Hours · Exam-Aligned Curriculum

Risk Mgmt — 16%

Assets — 10%

Architecture — 13%

Networks — 13%

IAM — 13%

Assessment — 12%

Operations — 13%

Software — 10%

In short: This is an instructor-led certification program mapped 1:1 to the official ISC2 CISSP Exam Outline (effective April 15, 2024) — the advanced, senior-level information security credential, ANAB-accredited under ISO/IEC 17024 and approved under U.S. DoD Directive 8140/8570. You master all eight domains, from security governance and risk management through architecture, networks, IAM, assessment, and operations to software development security — with AI/ML security interwoven across every domain (securing training data and models, defending against adversarial attacks and prompt injection, using AI for defensive automation), exactly as the current outline treats it. The program closes with full-length CAT-format mock exams. On completion you are ready to pass the CISSP and step into senior security leadership and architecture roles.

Certification	CISSP — Certified Information Systems Security Professional	Offered by	ISC2
Level	Advanced / senior-level information security certification	Accreditation	ANAB ISO/IEC 17024; U.S. DoD Directive 8140/8570 approved
Experience	Minimum 5 years cumulative, full-time professional work experience in 2+ of the 8 domains; a relevant degree or approved ISC2 credential may waive up to 1 year (max 1 year). Without it: pass the exam as an Associate of ISC2, then earn the 5 years within 6 years.		
Format	Computerized Adaptive Testing (CAT); 100–150 items incl. advanced types (drag-and-drop, hotspot)	Length	3 hours
Passing score	700 out of 1000 points	Languages	English, Chinese, German, Japanese, Spanish
Delivery	ISC2 Authorized Pearson VUE Testing Centers	Maintenance	Valid 3 years; maintained via CPE credits

Domain 1: Security and Risk Management

16%

ESTIMATED TIME

7–8 Hours

TOPICS

- Professional ethics (ISC2 Code of Ethics; organizational codes)
- Core security concepts: the 5 pillars — confidentiality, integrity, availability, authenticity, and nonrepudiation
- Security governance principles; alignment to business strategy; control frameworks (ISO, NIST, COBIT, SABSA, PCI, FedRAMP); due care / due diligence
- Legal, regulatory, and compliance issues; cybercrime and data breaches; IP and licensing; import/export controls; transborder data flow; privacy (GDPR, CCPA, etc.)
- Investigation types (administrative, criminal, civil, regulatory, industry standards)
- Security policies, standards, procedures, and guidelines
- Business Continuity (BC) requirements and Business Impact Analysis (BIA)
- Personnel security policies (screening, agreements, onboarding/transfer/termination)
- Risk management concepts (threat/vulnerability ID, risk analysis and treatment, control types, continuous monitoring, risk frameworks)
- Threat modeling; Supply Chain Risk Management (SCRM)
- Security awareness, education, and training programs

HANDS-ON

- Run a BIA and build a risk register for a case-study organization
- Threat-model a system including AI/ML components

Assessment: Quiz + Scenario Exercise

Domain 2: Asset Security

10%

ESTIMATED TIME

4–5 Hours

TOPICS

- Identify and classify information and assets (data and asset classification)
- Establish information and asset handling requirements
- Provision information and assets securely (ownership, inventory, asset management)
- Manage the data lifecycle (data roles, collection, location, retention, remanence, destruction)
- Ensure appropriate asset retention (EOL, End of Support)
- Determine data security controls and compliance requirements (data states, scoping and tailoring, standards selection, DRM/DLP/CASB)

HANDS-ON

- Build a data classification and handling matrix for a case study
- Map lifecycle controls from collection through destruction

Assessment: Quiz

Domain 3: Security Architecture and Engineering

13%

ESTIMATED TIME

6–7 Hours

TOPICS

- Secure design principles (least privilege, defense in depth, secure defaults, fail securely, SoD, zero trust, privacy by design, shared responsibility, SASE)
- Security models (Biba, Bell-LaPadula, Star Model)
- Select controls based on systems security requirements
- Security capabilities of information systems (memory protection, TPM, encryption)
- Assess/mitigate vulnerabilities of architectures (client/server, databases, cloud, ICS, IoT, microservices, containerization, serverless, embedded, edge, virtualized)
- Cryptographic solutions and lifecycle (symmetric/asymmetric, elliptic curve, quantum, PKI); cryptanalytic attacks (brute force, side-channel, MITM, pass-the-hash, ransomware)
- Site and facility security design (data centers, HVAC, fire suppression, power)
- Information system lifecycle management

HANDS-ON

- Design a zero-trust architecture for a hybrid estate
- Select cryptographic solutions and defend against adversarial AI attacks

Assessment: Quiz + Design Exercise

Domain 4: Communication and Network Security

13%

ESTIMATED TIME

6–7 Hours

TOPICS

- Secure network architecture design (OSI and TCP/IP models, IPv4/IPv6, secure protocols IPSec/SSH/TLS, converged and multilayer protocols)
- Segmentation (physical, logical, micro-segmentation), edge/wireless/cellular networks, CDNs, SDN, VPC, network monitoring and management
- Secure network components (infrastructure operation, transmission media, NAC, endpoint security)
- Secure communication channels (voice/video/collaboration, remote access, data comms, third-party connectivity)

HANDS-ON

- Design a segmented network with secure protocols and NAC
- Evaluate remote access and third-party connectivity risks

Assessment: Quiz**Domain 5: Identity and Access Management (IAM)****13%****ESTIMATED TIME**

6–7 Hours

TOPICS

- Control physical and logical access to assets (information, systems, devices, facilities, applications, services)
- Identification and authentication strategy (AAA, MFA, passwordless, session management, FIM, credential management, SSO, Just-In-Time)
- Federated identity with third-party services (on-premises, cloud, hybrid)
- Authorization mechanisms (RBAC, rule-based, MAC, DAC, ABAC, risk-based, policy enforcement)
- Identity and access provisioning lifecycle (access review, provisioning/deprovisioning, role transition, privilege escalation, service account management)
- Implement authentication systems

HANDS-ON

- Design an MFA + SSO strategy with federated identity
- Walk an identity through the full provisioning lifecycle

Assessment: Quiz**Domain 6: Security Assessment and Testing****12%****ESTIMATED TIME**

5–6 Hours

TOPICS

- Design and validate assessment, test, and audit strategies (internal, external, third-party)
- Conduct security control testing (vulnerability assessment, penetration testing / red-blue-purple teams, log reviews, code review, misuse case testing, interface testing, breach attack simulations, compliance checks)
- Collect security process data (account management, KPIs/KRIs, backup verification, training, DR/BC)
- Analyze test output and generate reports (remediation, exception handling, ethical disclosure)
- Conduct or facilitate security audits (internal, external, third-party)

HANDS-ON

- Plan a penetration test and interpret its findings report
- Build a KPI/KRI dashboard for a security program

Assessment: Quiz**Domain 7: Security Operations****13%****ESTIMATED TIME**

6–7 Hours

TOPICS

- Investigations (evidence collection/handling, reporting, digital forensics, artifacts)
- Logging and monitoring (IDPS, SIEM, continuous monitoring, egress monitoring, threat intelligence and hunting, UEBA)
- Configuration Management; foundational operations concepts (need-to-know/least privilege, SoD, privileged account management, job rotation, SLAs)
- Resource protection; incident management (detection, response, mitigation, reporting, recovery, remediation, lessons learned)
- Detective and preventative measures (firewalls, IDS/IPS, sandboxing, honeypots, anti-malware, ML/AI-based tools); patch and vulnerability management; change management
- Recovery strategies; Disaster Recovery (DR) processes and testing; BC planning
- Physical security; personnel safety and security (travel, duress, emergency management)

HANDS-ON

- Run an incident response tabletop from detection to lessons learned
- Design a DR test plan with SIEM-driven monitoring

Assessment: Quiz + Tabletop Exercise

Domain 8: Software Development Security

10%

ESTIMATED TIME

4–5 Hours

TOPICS

- Integrate security into the SDLC (Agile, Waterfall, DevOps, DevSecOps; maturity models CMM/SAMM; change management)
- Security controls in development ecosystems (languages, libraries, toolsets, IDE, CI/CD, code repositories, application security testing — SAST, DAST, IAST, SCA)
- Assess effectiveness of software security (auditing/logging of changes, risk analysis)
- Assess security impact of acquired software (COTS, open source, third-party, managed and cloud services)
- Define and apply secure coding guidelines and standards (source-code weaknesses, API security, secure coding practices, software-defined security)

HANDS-ON

- Thread security gates (SAST/DAST/SCA) into a CI/CD pipeline
- Review code and APIs against secure coding standards — including prompt-injection defenses

Assessment: Quiz

Exam Readiness & Mock Exams**ESTIMATED TIME**

4–5 Hours

TOPICS

- CAT mechanics and strategy; advanced item types (drag-and-drop, hotspot); pacing for 100–150 items in 3 hours
- Domain-by-domain review keyed to the official weightings; risk-first, business-aligned reasoning
- Certification path: experience requirement, the 1-year waiver, the Associate of ISC2 route; 3-year CPE maintenance cycle

HANDS-ON

- Full-length CAT-style mock exams with detailed rationales
- Weak-domain drills and final review

Assessment: Mock Exams