

CISSP Exam Tutoring Bootcamp

Course Overview:

A 3-day, exam-focused bootcamp that reviews all eight CISSP domains, explains the concepts the exam tests most, and drills the reasoning techniques candidates need to pass the adaptive exam through practice exam questions.

Course Objective:

This course is designed for security professionals who have already studied or experience in the CISSP domains and plan to sit the exam within 2–6 weeks. This is an accelerator and tutoring course, not a first-time introduction.

Prerequisites:

Participants should have completed a full CISSP 5 days training course or self-study through official study guide or equivalent and already practice through official practice exam questions or equivalent with an average first time correct answer of 60% or more.

By the end of the course, participants will be able to:

- Explain the core concepts of each domain in plain language and connect them across domains.
- Answer short scenario-based questions from a manager's and risk advisor's perspective, not a technical.
- Apply a repeatable question-deconstruction method to eliminate distractors.
- Pace a 100–150 question adaptive exam within 3 hours without second-guessing.
- Identify their own weak domains from a full mock exam and follow a targeted final study plan.

Delivery format:

Every domain runs in two parts. First, a 10–20 minute domain summary covering only the key concepts, terms and memory aids. Then a question walkthrough for the rest of the domain's time: participants answer each exam-style question first, then the tutor explains why the correct answer is right, why each distractor is wrong, and the concept behind it. Questions run from foundational to hard scenario items, so the domain is taught through the practice exam questions.

Exam at a glance:

The current CISSP exam outline took effect on 15 April 2024: an adaptive (CAT) exam of 100–150 items in a maximum of 3 hours, with a passing score of 700 out of 1000. Certification also requires 5 years of cumulative paid experience in two or more domains; passing without it earns Associate of ISC2 status.

Bootcamp time is allocated roughly in proportion to domain weight, with extra time on Domains 1 and 3 because their concepts are foundations of every other domain.

Domain	Exam weight	Bootcamp day	Summary	Question walkthrough
1. Security and Risk Management	16%	Day 1	20 min	2 h 5 min (~45 questions)
2. Asset Security	10%	Day 1	15 min	1 h 15 min (~20 questions)
3. Security Architecture and Engineering	13%	Day 1	15 min	1 h 5 min (~25 questions)
4. Communication and Network Security	13%	Day 2	15 min	1 h 35 min (~35 questions)
5. Identity and Access Management	13%	Day 2	15 min	1 h 55 min (~35 questions)
6. Security Assessment and Testing	12%	Day 2	15 min	1 h 5 min (~20 questions)
7. Security Operations	13%	Day 3	15 min	1 h 25 min (~30 questions)
8. Software Development Security	10%	Day 3	10 min	45 min (~20 questions)

Course Outline:

Day 1 – Governance, assets and architecture (Domains 1–3)

Sets the mindset the whole exam rewards – security supports the business and risk decisions belong to senior management – and teaches it through about 100 explained questions.

Techniques introduced: the "manager first" filter, risk-formula drills, and the security-model memory grid (e.g. which model protects confidentiality vs integrity, and which rule is "no read up" vs "no write down").

Estimate course agenda for Day 1 are as follows:

Session	Content
Kick-off and exam orientation	CAT mechanics, scoring, test-day logistics; "think like a manager" introduction; how the question walkthroughs work; review of baseline scores
Domain 1 summary	Ethics canons; due care vs due diligence; governance roles; policy hierarchy; legal and privacy; risk frameworks and formulas (AV, EF, SLE, ARO, ALE); control types; BCP/BIA terms (RTO, RPO, MTD)
Domain 1 questions, part 1	~20 questions on ethics, governance, legal, regulatory and privacy scenarios, each with full answer and distractor explanation
Break	

Session	Content
Domain 1 questions, part 2	~25 questions on risk analysis (including worked ALE calculations), risk responses, BCP/BIA, supply chain and awareness
Lunch	
Domain 2 summary	Classification and labelling; data roles (owner, controller, processor, custodian); data lifecycle, states and retention; sanitization methods; scoping and tailoring
Domain 2 questions	~20 questions with explanation, focused on choosing the right data role, classification and destruction method
Break	
Domain 3 summary	Secure design principles; security models (Bell–LaPadula, Biba, Clark–Wilson, Brewer–Nash); cryptography and PKI; system vulnerabilities (cloud, IoT, ICS); physical security
Domain 3 questions	~25 questions with explanation: design principles, model rules, choosing crypto for confidentiality vs integrity vs non-repudiation, key management, facility controls
Mixed recap	10 cross-domain questions on Domains 1–3, answered under time pressure, then explained
Wrap-up	Homework: 50 practice questions on Domains 1–3

*May be changed based on situations during course delivery

Day 2 – Networks, identity and testing (Domains 4–6)

Covers the most technical material through about 100 explained questions, and each explanation translates the technology back into a business or risk decision.

Techniques introduced: the OSI and TCP/IP model "layer anchor" (place every protocol and attack on a layer before answering), keyword triggers for access control models, and "who should receive the report" reasoning for audit questions.

Estimate course agenda for Day 2 are as follows:

Session	Content
Day 1 homework review	Most-missed homework questions, explained
Domain 4 summary	OSI vs TCP/IP layers and what lives at each; secure protocols (TLS, IPsec, SSH, SNMPv3); segmentation and zero trust; firewalls, IDS/IPS, VPNs; wireless security; SDN, CDN and cloud networking
Domain 4 questions, part 1	~20 questions with explanation on layers, protocols, ports and network attacks
Break	

Session	Content
Domain 4 questions, part 2	~15 questions on secure network design, wireless, remote access and cloud scenarios
Domain 5 summary	Identification, authentication, authorisation, accountability; MFA and biometrics (FRR, FAR, CER); access control models (DAC, MAC, RBAC, ABAC); federation and SSO (SAML, OAuth, OIDC, Kerberos); identity lifecycle
Domain 5 questions, part 1	~10 questions on authentication factors, biometrics and access control models
Lunch	
Domain 5 questions, part 2	~25 questions on federation, SSO, provisioning, access reviews and privilege creep
Break	
Domain 6 summary	Audit strategy and SOC reports (Type I vs II); vulnerability scan vs pen test; black, grey, white box; code testing (static, dynamic, fuzzing); KPIs and KRIs; reporting to management
Domain 6 questions	~20 questions with explanation, focused on choosing the right test, the right report and who should receive it
Mixed recap	10 cross-domain questions on Domains 1–6, then explained
Wrap-up	Homework: 50 practice questions on Domains 4–6

*May be changed based on situations during course delivery

Day 3 – Operations, software security and exam readiness (Domains 7–8 + mock exam)

Finishes Domains 7 and 8 by midday with about 50 explained questions, then spends the afternoon on a full mock exam and turning its results into a personal final-week plan.

Techniques introduced: the incident response sequence drill, "what is the FIRST / BEST / MOST important" question patterns, and the mock-exam domain heat map used to target final study.

Estimate course agenda for Day 3 are as follows:

Session	Content
Day 2 homework review	Most-missed homework questions, explained
Domain 7 summary	Investigations and evidence (chain of custody, order of volatility); logging, SIEM and monitoring; change and patch management; incident response lifecycle; backups and recovery sites; DR test types; personnel safety first
Domain 7 questions, part 1	~20 questions with explanation on incident response order, investigations, evidence and monitoring
Break	
Domain 7 questions, part 2	~10 questions on recovery sites, DR testing and change management

Session	Content
Domain 8 summary	Secure SDLC; agile and DevSecOps; maturity models (CMMI, SAMM); OWASP weaknesses; API and database security; third-party and open-source software risk
Domain 8 questions	~20 questions with explanation on SDLC phases, secure coding, database issues and software acquisition
Lunch	
Mock exam	75 questions in 90 minutes (exam pace of about 72 seconds per question), weighted to the exam outline; no going back on answers, to simulate CAT conditions. The full 150-question mock is provided as self-practice (1 month access)
Break	
Mock exam debrief	Score by domain; walkthrough of the 15–20 most-missed questions with full explanation
Exam strategy and test-day rehearsal	Pacing plan, mental reset routine, test-centre procedures, final "think like a manager" review
Personal study plan and close	Each participant writes a 2–3 week plan from their domain scores; course evaluation

*May be changed based on situations during course delivery

Exam techniques you will gain:

These techniques are taught and practiced on every question set, so by the mock exam they are habits, by muscle memory. They are your guts rather than notes.

1. Think like a manager and risk advisor
2. Question deconstruction
3. Spot common distractors
4. Use the process order
5. Pace the CAT exam
6. Manage mental energy

Materials, assessment and post-course plan:

Participant materials

- Domain summary handouts
- Formula and memory-aid sheet: risk calculations, BCP metrics, security models, OSI layers, IR and SDLC sequences
- Practice question bank of about 500 items, mapped to the 2024 outline (250 questions are taught and drilled through the course)
- Full 150 questions mock exam with domain-level scoring (75 questions are mock exam tested on the last day of the course)
- Recommended references: the official ISC2 CISSP study guide and official practice tests (recommendation only, not provided as part of the course)

Course assessment structure:

Checkpoint	When	Purpose
Baseline practice test	Before Day 1	50 Questions Pre-test Set starting point and group weak areas
Domain walkthroughs and mixed recaps	Throughout Days 1–3	Check understanding and technique use
Full mock exam	Day 3 afternoon	Readiness indicator; target 75%+ before booking the exam
Create personal self-study plan	Day 3 close	Turn domain scores into focused final study

Who should attend?

This bootcamp is designed for experienced security professionals who have already studied the CISSP material and want a fast, exam-focused push to be ready to sit the exam.

Typical roles those would gain benefit from this course are:

- Security managers, CISOs and heads of information security
- Security architects, engineers and analysts
- IT and network managers moving into security leadership
- IT auditors, risk and compliance managers, and GRC specialists
- Security consultants and SOC leads

You will get the most from this course if you:

- Have, or are working towards, 5 years of cumulative paid experience in at least two of the eight CISSP domains (candidates who pass without it can become an Associate of ISC2)
- Have finished at least one full pass through an official study guide or a full-length CISSP course
- Score around 60% or more on practice tests and plan to sit the exam within 2–6 weeks
- Want to sharpen exam technique and fill specific gaps rather than learn the domains from scratch

This course is not the right fit if you:

- Are new to information security, or have not yet studied the eight domains, A full 5-day CISSP training course is a better first step
- Are looking for hands-on technical labs — this course is built around exam-style questions and explanation, not practical tool work. Also hands-on labs are not part of CISSP exam requirements

Course Duration

3 days

For More Information Please Contact: Vnohow (Thailand) Co., Ltd.

90/31 Sathorn Thani Building 1, 12FL, North Sathorn Road, Silom, Bangrak, Bangkok 10500 Thailand
Tel +662-634-3287-9, +662-634-3299 Email vnohow@vnohow.com Website www.vnohow.com