
# (ISC)²-CISSP-CBK Official Bootcamp

**The Official (ISC)² Preparation Course to ace your CISSP exam**

**Offered by See Secuity College**

CISSP is often referred to as the "gold standard" of security certifications and serves as a professional checkpoint for any cybersecurity expert. CISSP is one of the most important distinctions you can have on your resume.

However, the certification is often perceived as very challenging, and many competent professionals are intimidated by it.

See Security is an official training partner of (ISC)² in Israel and deliver official preparation bootcamps for over 8 years. We offer the preparation bootcamp with authorised lecturers, official (ISC)² study material and years of experience.

Step by step, we will teach you what you **need to know** for the exam, guide you through the study materials for your home revision, and accompanied you once you clear the exam and begin the endorsement process.


# (ISC)²-CISSP-CBK Official Bootcamp

**A unique preparation programme offered by See Security College for advanced cybersecurity professionals who wish to accredit their knowledge by attempting the prestigious CISSP examination.**

## About See Security College

See Security College is a highly specialised and international cybersecurity college. Our college offers training programmes aimed for absolute beginners to more advanced professionals. The college delivers its study programmes worldwide, through the See Security International brand as well as well-known governmental and special cybersecurity agencies.

See-Security CEO, Mr. Avi Weissman is one of the leaders of the Israeli Cyber industry and serves as an advisor and commentator to the Israeli government for the regulation of cyber professions. Further, Mr. Weissman was the co-founder of the Israeli Forum for Information Security (IFIS) together with Maj. Gen. (Res.) and former head of National Security Council, Yaakov Amidror. In addition to his role in leading the college, Avi is also a co-CEO of a cyber human resources company, See-HR and a cybersecurity consulting company, See Events – Managed SIEM/SOC.

## About (ISC)²

(ISC)² was founded in 1989. The founders saw the need for standardization and certification in the cybersecurity industry. Since then, founders and members have been shaping the information security profession.

(ISC)² is an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. More than 150,000 certified members strong, we empower professionals who touch every aspect of information security.

| Bootcamp Key Features | |
|---|---|
| **Cost** | 8,000 NIS (tax included, not including exam fees) |
| **Aaudience** | Advanced, experienced cybersecurity professionals |
| **Orientation** | Theoretical and applicative knowledge |
| **Objectives** | To review the essential knowledge outline in the official CISSP-CBK Domains, and to maximase preparedness for the CISSP certification. |
| **Entry requirements** | Practical knowledge in OS, networking, and cybersecurity technologies; practical experience in cyberesec methodologies and architecture. |
| **Certifications** | CISSP (registering to the exam is the responsibility of the student) |
| **Academic hours** | Total of 40 online training sessions |
| **Homework** | Total of 320 homework assignments |
| **Course format** | Online lectures accompanied with 1-on-1 session with the lecturers |

## About the (ISC)²-CISSP

**The Certified Information Systems Security Professional (CISSP)** is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

This cybersecurity certification is an elite way to demonstrate your knowledge, advance your career and become a member of a community of cybersecurity leaders. It shows you have all it takes to design, engineer, implement and run an information security program. The CISSP is an objective measure of excellence. It's the most globally recognized standard of achievement in the industry. And this cybersecurity certification was the first information security credential to meet the strict conditions of ISO/IEC Standard 17024.

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 8 domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

## Experience Requirements

Candidates must have a minimum of 5 years cumulative paid full-time work experience in 2 or more of the 8 domains of the CISSP CBK. Earning a 4-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience. A candidate that doesn't have the required experience to become a CISSP may become an Associate of (ISC)² by successfully passing the CISSP examination. The Associate of (ISC)² will then have 6 years to earn the 5 years required experience.

## CISSP Key Features

The CISSP exam uses Computerized Adaptive Testing (CAT) for all English exams. CISSP exams in all other languages are administered as linear, fixed-form exams.

| Exam Key Features | |
|---|---|
| **Duration** | 3 hours |
| **Number of questions** | 100 – 150 |
| **Question format** | Multiple choice and advanced innovative questions |
| **Passing grade** | 700 out of 1000 points |
| **Exam language availability** | English |
| **Testing center** | (ISC)2 Authorized PPC and PVTC Select Pearson VUE Testing Centers |

## CISSP Computerized Adaptive Testing

(ISC)² has introduced Computerized Adaptive Testing (CAT) for all English CISSP exams worldwide. Based on the same exam content outline as the linear, fixed-form exam, CISSP CAT is a more precise and efficient evaluation of your competency. CISSP CAT enables you to prove your knowledge by answering fewer items and completing the exam in half the time.

### How Does it Work?

Each candidate taking the CISSP CAT exam will start with an item that is well below the passing standard. Following a candidate's response to an item, the scoring algorithm re-estimates the candidate's ability based on the difficulty of all items presented and answers provided. With each additional item answered, the computer's estimate of the candidate's ability becomes more precise – gathering as much information as possible about a candidate's true ability level more efficiently than traditional, linear exams. This more precise evaluation enables us to reduce the maximum exam administration time from 6 hours to 3 hours,

and it reduces the items necessary to accurately assess a candidate's ability from 250 items on a linear, fixed-form exam to as little as 100 items on the CISSP CAT exam. The exam content outline and passing standard for both versions of the examination are exactly the same. Each candidate will be assessed on the same content and must demonstrate the same level of competency regardless of the exam format. CISSP exams in all other languages, as well as all CISSP concentration exams are delivered as linear, fixed-form exams.

## CISSP Training Course Overview

Our training helps you fully prepare for this cybersecurity certification. You will:

(a) Review, refresh and expand your information security knowledge (including information security concepts and industry best practices).
(b) Identify areas you need to study for the CISSP exam.

You can expect an in-depth review of the eight domains of the CISSP CBK — including discussion of industry best practices and timely security concepts. (ISC)² authorized instructors lead all our training. You're learning from CISSP-certified industry experts who understand you. They are CISSPs themselves. They know how to make the content highly relatable. And they go through a rigorous process to teach to (ISC)² CBK.

## Study Materials

The following materials are included in the official student's kits.

(a) **Official (ISC)² Guide to the CISSP CBK**. The Official (ISC)² Guide to the CISSP CBK, Fifth Edition provides a comprehensive study of the refreshed eight domains. This book covers the most current topics in the information security industry today and includes numerous illustrated examples and practical exercises are included in this book to demonstrate concepts and real-life scenarios
(b) **162 Assessment Questions.** These questions are intended to assess your knowledge and progress, as part of your preparation for test-day

## Examination Policies and Procedures

(ISC)² recommends that CISSP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

## Our Lecturers

Such a multi-disciplinary programme requires uncompromising and dedicated experts. The lecturers include industry cybersecurity leaders, renowned CISOs, and leading professional experts in their respective field. You are learning from CISSP-certified industry experts who understand you. They are CISSPs themselves. They know how to make the content highly relatable. And they go through a rigorous process to teach to (ISC)² CBK.

## Requirements

You will not be tested on these requirements for enrolment. However, we emphasize that without background knowledge it will be difficult to keep up with materials covered throughout the course and even more challenging to pass the exams and assignments. The following are required:

a. Practical knowledge and experience in IT systems and networking.
b. Familiarity and experience with cybersecurity solutions and products technologies and methodologies.

**Or:**

a. BSc (or equivalent) in Computer Science or Software Engineering and / or graduation from a recognised CISO programme.

## Domain 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics
- Understand and apply security concepts
- Evaluate and apply security governance principles
- Determine compliance and other requirements
- Understand legal and regulatory issues that pertain to information security in a holistic context
- Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

## Domain 2: Asset Security

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
- Determine data security controls and compliance requirements

## Domain 3: Security Architecture and Engineering

- Research, implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
- Select controls based upon systems security requirements
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modelling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
- Establish and maintain a security awareness, education, and training program
- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Select and determine cryptographic solutions
- Understand methods of cryptanalytic attacks
- Apply security principles to site and facility design
- Design site and facility security controls

## Domain 4: Communication and Network Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design


## Domain 5: Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

## Domain 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

## Domain 7: Security Operations

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

## Domain 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards