(ISC)² CISSP– Certified Information Systems Security Professional

What is CISSP?

The Certified Information Systems Security Professional (CISSP) course is designed for information technology (IT) security professionals who intend to gain the necessary knowledge and certification based on the International Information System Security Certification Consortium (ISC)² curriculum and requirements to play a leading professional role in the employment workforce and career.

LearnersOne's official CISSP training course reviews the eight CISSP certification domains featured in the (ISC)² Common Body of Knowledge (CBK). Reviewing the CBK will help students successfully prepare for the CISSP exam while also develop their overall competencies in information security.

Course Breakdown

Domain 1	Security and Risk Management
Domain 2	Asset Security
Domain 3	Security Architecture and Engineering
Domain 4	Communication and Network Security
Domain 5	Identity and Access Management (IAM)
Domain 6	Security Assessment and Testing
Domain 7	Security and Operations
Domain 8	Software Development Security

https://learnersone.com
(240) 930-4053

Table of **Contents:**

Program **Overview:**

CISSP certification training develops your expertise in defining IT architecture and designing, building, and maintaining a secure business environment using globally approved information security standards. This course covers industry best practices and prepares you for the CISSP certification exam held by (ISC).

Program **Features:**

- 67 hours of blended learning
- 35 hours of online self-paced learning
- 48 hours of instructor led training
- Five simulation test papers to prepare you for CISSP certification
- Offers the requisite 30 CPEs for taking the CISSP examination
- CISSP exam voucher

Delivery **Mode:**

Blended - Online self-paced learning and live virtual classroom

Prerequisites:

Candidates must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Earning a four-year college degree or regional equivalent or an additional credential from the (ISC)2 approved list will satisfy one year of the required experience. Education credit will only satisfy one 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 six years to earn the five years required experience.

Target **Audience:**

The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions:

- Chief Information Security Officer
- Chief Information Officer
- Director of Security IT
- Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant
- Network Architect

Key Learning **Outcomes:**

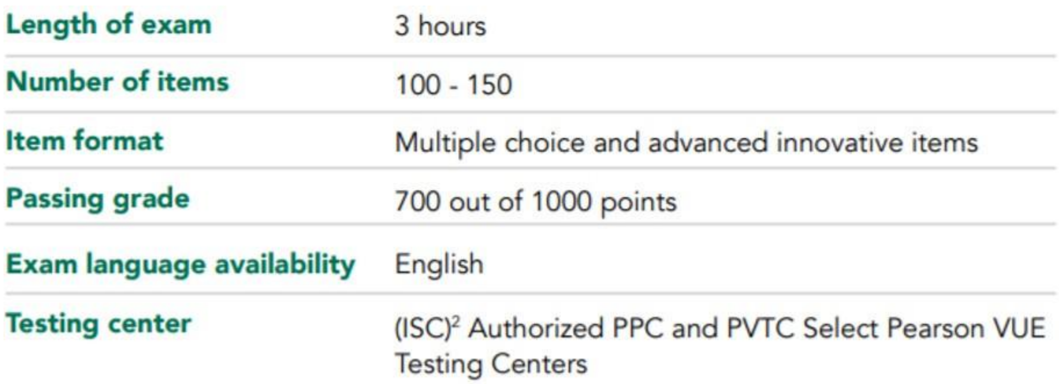
By the end of this CISSP training, you will:

- Be able to define the architecture, design, and management of the security of your organization
- Acquire the relevant knowledge and skills required to pass the CISSP certification exam
- Perform risk analysis and prevent data loss
- Learn about security architecture, engineering, models, and cryptography
- Gain familiarity with communications and network security, identity and access management, and security testing and operations

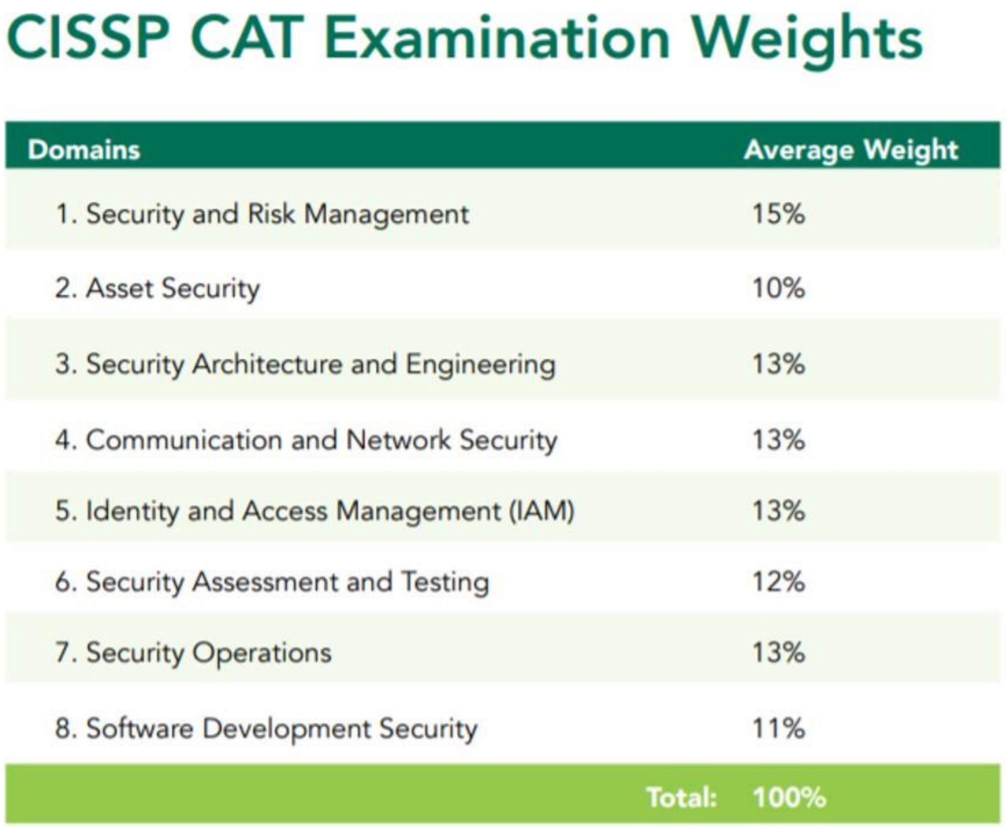
Exam **Details:**

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.

1. CISSP CAT Examination Information



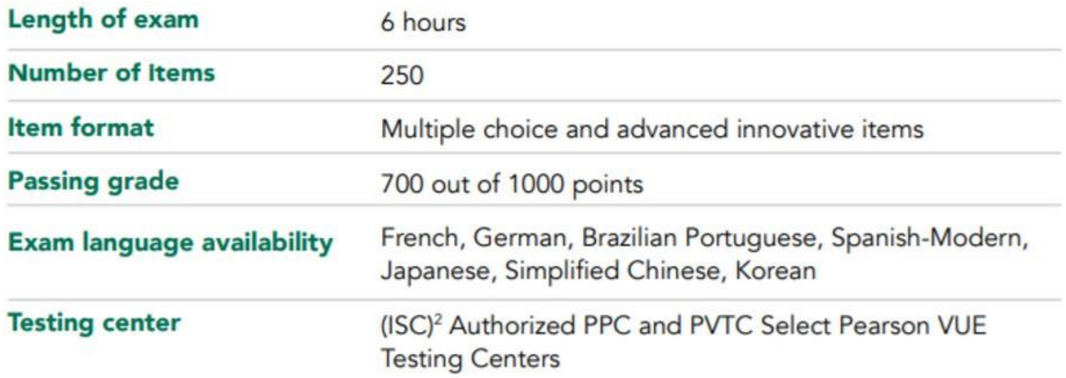
Length of exam	3 hours
Number of items	100 - 150
Item format	Multiple choice and advanced innovative items
Passing grade	700 out of 1000 points
Exam language availability	English
Testing center	(ISC)^2 Authorized PPC and PVTC Select Pearson VUE Testing Centers



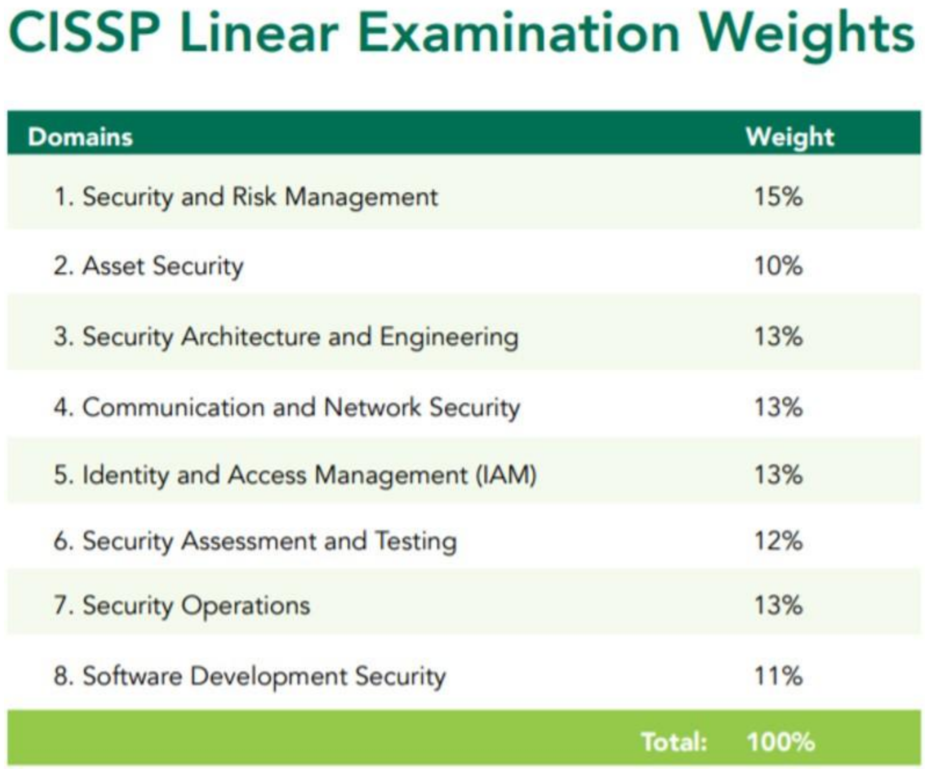
CISSP CAT Examination Weights

Domains	Average Weight
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	13%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	11%
Total:	**100%**

2. CISSP Linear Examination Information



Length of exam	6 hours
Number of Items	250
Item format	Multiple choice and advanced innovative items
Passing grade	700 out of 1000 points
Exam language availability	French, German, Brazilian Portuguese, Spanish-Modern, Japanese, Simplified Chinese, Korean
Testing center	(ISC)^2 Authorized PPC and PVTC Select Pearson VUE Testing Centers



CISSP Linear Examination Weights

Domains	Weight
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	13%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	11%
Total:	**100%**

LearnersOne Course **Completion Criteria-**

Onsite/Online Classroom:

- Attend one complete batch
- Complete one simulation test with a minimum score of 60 percent

Online Self-Learning:

- Complete 85 percent of the course
- Complete one simulation test with a minimum score of 60 percent

Course **Curriculum:**

Lesson 01 - Course Introduction

- Course Introduction

Lesson 02 - Security and Risk Management

- Security and Risk Management Information
- Security Management Security Controls
- Information Security Management and Governance Goals,
- Mission, and Objectives
- Due Care Security
- Policy Compliance
- Computer Crimes
- Legal Systems
- Intellectual Property (IP) Law
- Privacy
- General Data Protection Regulation Security
- Risk Analysis
- Types of Risk Analysis Security
- Control Assessment Threat
- Modeling
- Supply-Chain Risk Management
- Third-Party Management Business
- Continuity Planning
- Business Continuity Planning Phases
- Managing Personnel Security
- Security Awareness Training Program
- Effectiveness Evaluation Key
- Takeaways
- Knowledge Check

Lesson 03 - Asset Security

- Asset Security
- Information Classification
- Data Classification
- Data Life Cycle
- Data Management
- Different Roles
- Data Remanence
- Privacy
- States of Data
- Data Loss Prevention
- Key Takeaways
- Knowledge Check

Lesson 04 - Security Engineering

- Introduction Security
- Engineering
- Security Architecture
- Security Models
- Evaluation Criteria
- System Security
- CPU
- Memory Security
- Mode
- Cloud Computing
- IoT
- Industrial Control System (ICS)
- Cryptography
- Encryption Methods
- DES
- Asymmetric Cryptography Public
- Key Infrastructure Cryptanalysis
- Key Management
- Critical Path Analysis
- Site Location
- Fire
- HVA
- Key Takeaways
- Knowledge Check

Lesson 05 - Communications and Network Security

- Introduction
- Network Architecture and Design
- IP Addressing
- Network Protocols
- Transmission Media
- Firewall
- Intrusion Detection System and Intrusion Prevention System Network
- Access Control (NAC)
- Content Delivery Network (CDN)
- Networks
- Software-Defined Networking (SDN)
- Remote Access
- Internet Security Protocol (IPsec)
- Voice over Internet Protocol (VoIP)
- Phreaking
- Secure Access Protocols
- Wireless Technologies
- Network Attacks
- Key Takeaways
- Knowledge Check

Lesson 06 - Identity and Access Management

- Identity and Access Management
- Identity Management
- Biometrics
- Passwords
- Tokens
- Memory Cards and Smart Cards
- Access and Authorization Concepts
- Identity Management Implementation
- Kerberos
- Access Control Types
- Access Control Models
- Access Control Tools and Techniques
- Accountability
- Access Control Monitoring
- Identity Proofing
- Markup Languages
- Identity as a Service (IDaaS)
- Key Takeaways

Lesson 09 - Software Development Security

- Software Development Security
- Importance of Software Development Security
- Programming Concepts
- Systems Development Life Cycle
- Application Program Interface
- Software Security and Assurance
- Database and Data Warehouse Environments
- Knowledge Management
- Web Application
- Environment Security Threats
- and Attacks Key Takeaways
- Knowledge Check

About **Us**:

Trusted by hundreds of satisfied students and organizations, we are a top-notch educator providing the most complete training complete training programs to help you stay informed, engaged and a step ahead.