Publication date : 02/25/2026

# Course : Certified Information Systems Security Professional (CISSP), preparation for ISC2 certification

**Official ISC2 training**

*Practical course - 5d - 35h00 - Ref. CIQ*

*Price : 4250 € E.T.*

NEW

This course covers the entire Common Body of Knowledge (CBK) defined by ISC2 and prepares you for the CISSP exam, the international benchmark in information systems security.

## Teaching objectives

**At the end of the training, the participant will be able to:**

- Design and manage a global information security program aligned with business objectives
- Identify, analyze, assess and manage cyber risks in a complex organizational context
- Define and implement security governance integrated with the organization's strategy
- Select and deploy safety controls adapted to operational and regulatory requirements
- Oversee security operations, incident management and business continuity
- Integrating security into IT architectures, networks and software development cycles
- Adopt the "manager/decision-maker" reasoning expected by ISC2 to pass the CISSP exam

## Intended audience

Managers, directors, architects, engineers, analysts, auditors and consultants involved in the security of information systems and network infrastructures. here

## Prerequisites

At least five years' cumulative professional experience in at least two of the eight areas of the ISC2 CISSP examination program.

**PARTICIPANTS**

Managers, directors, architects, engineers, analysts, auditors and consultants involved in the security of information systems and network infrastructures. here

**PREREQUISITES**

At least five years' cumulative professional experience in at least two of the eight areas of the ISC2 CISSP examination program.

**TRAINER QUALIFICATIONS**

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

**ASSESSMENT TERMS**

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

## Practical details

Please enter the practice description here

## Course schedule

### 1 Area 1: Safety and risk management

- Professional ethics and Code of Ethics ISC2.
- Fundamentals of information security.
- Safety governance and organizational roles.
- Regulatory compliance and legal frameworks.
- Legal, regulatory and contractual issues.
- Types of surveys and associated processes.
- Safety policies, standards, procedures and guidelines.
- Business continuity and business impact analysis (BIA).
- Human resources security.
- Risk management: identification, analysis, treatment.
- Threat modeling.
- Supply chain risk management.
- Awareness, training and safety culture.

### 2 Area 2: Asset safety

- Asset identification and classification.
- Ownership and responsibility for information.
- Data protection requirements.
- Data lifecycle management.
- Secure storage, archiving and destruction.
- Security checks and data compliance.

### 3 Area 3: Security architecture and engineering

- Principles of safe design and engineering.
- Safety mode and basic concepts.
- Selection of system security controls.
- Security of hardware and software components.
- Vulnerability of architectures and designs.
- Cryptography: principles, uses and governance.
- Cryptographic threats and attacks.
- Physical security of sites and infrastructures.

### 4 Area 4: Communications and network security

- Principles of secure network design.
- Securing network equipment and infrastructure.
- Segmentation, isolation and defense in depth.
- Secure communication channels.

### 5 Area 5: Identity and access management (IAM)

- Physical and logical access control.
- Identification and authentication.
- Identity federations and third-party services.
- Authorization and rights management.
- Identity and access lifecycle.
- Authentication mechanisms.

**TEACHING AIDS AND TECHNICAL RESOURCES**

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.

• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.

• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

**TERMS AND DEADLINES**

Registration must be completed 24 hours before the start of the training.

**ACCESSIBILITY FOR PEOPLE WITH DISABILITIES**

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

### 6 Area 6: Safety assessment and testing

- Security testing and auditing strategies.
- Technical and organizational tests.
- Collecting and analyzing results.
- Writing safety reports.
- Internal and external audits.

### 7 Area 7: Safety operations

- Surveys and investigations.
- Logging and monitoring.
- Configuration management.
- Daily safety operations.
- Protecting resources.
- Security incident management.
- Detection and prevention.
- Vulnerability management and patching.
- Change management.
- Business continuity and disaster recovery.
- Physical and environmental safety.
- Personnel safety.

### 8 CISSP exam preparation

- CISSP (CAT) exam presentation.
- Methodology for answering questions.
- Time management and common pitfalls.
- Assessment quizzes and exam-style questions.
- Advice from CISSP-certified experts.

## Options

**Certification : 750 € HT**

The official exam is a 3-hour multiple-choice test in English, with 100 to 150 questions, and a minimum score of 700/1000.

## Dates and locations

**REMOTE CLASS**
2026 : 15 June, 31 Aug., 2 Nov.

**PARIS LA DÉFENSE**
2026 : 15 June, 31 Aug., 2 Nov.