

## Certified Information Systems Security Professional (CISSP)



**Course Duration** : 5 days

### Course Overview

#### SPECIAL NOTICE

The CISSP course is not delivered as a boot camp or exam prep course. Our course is a 'theory based' guide through the eight ISC2 domains to support your learning of the ISC2 Book of Knowledge. This course should be taken many months in advance of your CISSP exam booking. It will not substitute the considerable amount of self-study that all CISSP delegates need to undertake. This course attracts mixed ability delegates and is always tailored to meet the needs of all participants.

Aimed at security professionals, this course surveys the entire information security landscape and the technologies involved. The course addresses the eight knowledge domains that comprise the common body of knowledge (CBK) for information systems security professionals and will help delegates prepare for CISSP certification.

The course offers a theory based approach to the security process, with opportunities to discuss the immediate application of concepts and techniques described in the CBK to the real world. It can be considered as providing a good introduction to security management, architecture and engineering.

The course comprises of eight sessions that map directly to the (CBK), each one is theory based with instructor led discussions; there are no hands on labs.

### Exams

This course will assist delegates preparing for the following exam: CISSP Certified Information Systems Security Professional.

To book the CBT exam requires the candidate to acquire a Pearson VUE testing voucher. Please note, the price of the voucher is not included in the RRP of this course

<https://www.isc2.org/certification-register-now.aspx>

### Continuous Professional Development (CPD)

- CPD points can be claimed for GCT accredited courses at the rate of 1 point per hour of training for GCHQ accredited courses (up to a maximum of 15 points).

### Prerequisites

- Delegates should have experience in at least two of the domains in the (CBK), for 5 years or more (4 years if they have achieved relevant industry or degree level certifications) to achieve full certification. Associate status can be achieved without the full 4/5 years' experience; full certification will be assigned when the correct amount of experience is obtained.
- We recommend delegates have some knowledge of all CBK domains and are encouraged to read one or two of the books on the Reading List at ISC2.org.
- We will provide a CISSP guide book as pre-reading. It is expected that delegates review the guide and gain an appreciation of the key concepts in each of the eight CISSP domains in advance of the course. However, we do not expect delegates to be familiar with all the details of the guide book in advance of the course itself.

- We recommend that work completed in the classroom is complemented by extra reading to ensure success in the exam. The amount of extra reading required will depend on the amount of experience the delegate has. The 'mile wide, inch deep' description indicates the challenge to most delegates, not all will have 'hands on' experience spanning all 8 domains of the CBK.

## Course Content

### Security and Risk Management

Understand and apply concepts of confidentiality, integrity and availability  
Apply security governance principles  
Compliance  
Understand legal and regulatory issues that pertain to information security in a global context  
Understand professional ethics  
Develop and implement documented security policy, standards, procedures, and guidelines  
Understand business continuity requirements  
Contribute to personnel security policies  
Understand and apply risk management concepts  
Understand and apply threat modelling  
Integrate security risk considerations into acquisition strategy and practice  
Establish and manage information security education, training, and awareness

### Asset Security

Classify information and supporting assets  
Determine and maintain ownership  
Protect privacy  
Ensure appropriate retention  
Determine data security controls  
Establish handling requirements

### Security Engineering

Implement and manage engineering processes using secure design principles  
Understand the fundamental concepts of security models  
Select controls and countermeasures based upon systems security evaluation models  
Understand security capabilities of information systems  
Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements  
Assess and mitigate the vulnerabilities in web-based systems  
Assess and mitigate vulnerabilities in mobile systems  
Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems  
Apply cryptography  
Apply secure principles to site and facility design  
Design and implement physical security

### Communication & Network Security

Apply secure design principles to network architecture  
Secure network components  
Design and establish secure communication channels  
Prevent or mitigate network attacks

### Identity & Access Management

Control physical and logical access to assets  
Manage identification and authentication of people and devices  
Integrate identity as a service  
Integrate third-party identity services  
Implement and manage authorization mechanisms  
Prevent or mitigate access control attacks  
Manage the identity and access provisioning lifecycle

### Security Assessment & Testing

Design and validate assessment and test strategies  
Conduct security control testing  
Collect security process data  
Analyse and report test outputs  
Understand the vulnerabilities of security architectures

### Security Operations

Understand and support investigations  
Understand requirements for investigation types  
Conduct logging and monitoring activities  
Secure the provisioning of resources  
Understand and apply foundational security operations concepts  
Employ resource protection techniques  
Conduct incident management  
Operate and maintain preventative measures

### Software Security Development

Understand and apply security in the software development lifecycle  
Enforce security controls in development environments  
Assess the effectiveness of software security  
Assess security impact of acquired software

**CISSP and CBK are registered certification marks of (ISC)2, Inc.**

## Training Options

- Public scheduled courses at one of our training venues
- Private courses delivered at client's premises throughout the UK, at our training venues or a convenient third-party location
- Bespoke customised courses written to your specific needs, delivered at client's premises throughout the UK, at our training venues or a convenient third-party location
- For further information please contact us on 0191 377 8377

## What's Included

- 1 delegate per computer
- Relaxed refreshment area at our training venues
- Comprehensive course materials, including pre-course reading