
CISSP Certified Information Systems Security Professional

| | |
|--------------------|-------|
| Days | 5 |
| Course code | CISSP |

Overview

Aimed at seasoned security professionals, this course surveys the entire information security landscape and the technologies involved.

The course addresses the ten knowledge domains that comprise the Common Body of Knowledge (CBK) for information systems security professionals and prepares delegates for CISSP certification. The course offers a job-related approach to the security process, demonstrating the immediate application of concepts and techniques described in the CBK and providing a basic introduction to security management, architecture and engineering.

The course comprises ten sessions that map directly to the (CBK), each one is theory based with instructor led discussions, there are no hands on labs. The work completed in the classroom should be complimented by extra reading, references to internet resources will be provided by the instructor.

Quote from (ISC)2 expressing who should take the CISSP certification:
“The CISSP credential is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.”

Prerequisites

Delegates should have experience of at least two of the domains in the (CBK), for 5 years or more (4 years if they have achieved relevant certifications, e.g., MCSE).

-
- Delegates must ensure that they 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.
 - Current requirements for the CISSP examination are to be found at ISC2.org.
-

Delegates will learn how to

This course will consolidate delegates' knowledge in:

-
- Access to information systems.
 - Network systems and telecommunications.
 - Security management.

-
- Applications security.
 - Cryptography.
 - Secure system architecture.
 - Operations security.
 - Business continuity planning.
 - Physical security.
 - Law, investigations, and ethics.
-

This course will assist delegates preparing for the following exam:

(ISC)2 – CISSP Certified Information Systems Security Professional

Course outline

Module 1: Access to Information Systems

Control Data Access
Control System Access
Determine an Access Control Administration Method
Perform a Penetration Test

Module 2: Networking Systems and Telecommunications

Design Data Networks
Provide Remote Access to a Data Network
Secure a Data Network
Manage a Data Network

Module 3: Security Management

Determine Security Management Goals
Classify Information
Develop a Security Program
Manage Risk

Module 4: Applications Security

Perform Software Configuration Management
Implement Software Controls
Secure Database Systems

Module 5: Cryptography

Apply a Basic Cipher
Select a Symmetric Key Cryptography Method
Select an Asymmetric Key Cryptography Method
Determine Email Security
Determine Internet Security

Module 6: Securing System Architecture

Evaluate Security Models

Choose a Security Mode
Provide System Assurance

Module 7: Operations Security

Control Operations Security
Audit and Monitor Systems
Handle Threats and Violations

Module 8: Business Continuity Planning

Sustain Business Processes
Perform Business Impact Analysis
Define Disaster Recovery Strategies
Test the Disaster Recovery Plan

Module 9: Physical Security

Control Physical Access
Monitor Physical Access
Establish Physical Security Methods
Design Secure Facilities

Module 10: Law, Investigations, and Ethics

Interpret Computer Crime Laws and Regulations
Apply the Evidence Life Cycle
Perform an Investigation
Identify Codes of Conduct