By the end of this cyber security training course, you should know and understand the key aspects of each of the 8 domains of CISSP which are:

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

Course Objectives

Gain the knowledge to become an Information Systems Security Professional with our CISSP course.

Our CISSP course lasts for 5 days and will help you succeed in a career of IS security. This course provides all the required knowledge to carry on and pass the CISSP exam. This CISSP training course is the main way to show and exhibit your understanding of information security and what is required of a security professional.

Having previous experience with IS security for around 5 years is highly advised or 4 years plus an IS University degree. If you don’t have this experience then you can become an Associate of (ISC)^2 which allows you to gain the necessary experience in the following 6 years instead.

Pre-course Reading

There is a book that is a requirement for participants to purchase before you start this course which is listed below.

Official (ISC)^2 Guide to the CISSP CBK, Fourth Edition (ISC2 Press) Hardcover by Adam Gordon (Editor)

ISBN-10: 1482262754

ISBN-13: 978-1482262759

Evening Work

The course will have exercises and tasks set for candidates to complete at home, this is to ensure that knowledge gained during each training session will be retained.

Exam

The entirety of the exam will be completed on a computer with a pass mark of 700/1000.

Security and Risk Management:

- Confidentiality, integrity, and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

Asset Security:

- Information and asset classification
- Ownership
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements

Security Engineering:

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Communication and Network Security:

- Secure network architecture design
- Secure network components
- Secure communication channels
- Network attacks

Identity and Access Management:

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service
- Third-party identity services
- Access control attacks

- Assessment and test strategies
- Security process data
- Security control testing
- Test outputs
- Security architectures vulnerabilities

Security Operations:

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Software Development Security:

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness

Acquired software security impact

Gain the knowledge to become an Information Systems Security Professional with our CISSP.

Our CISSP course lasts for 5 days and will help you succeed in a career of IS security. This course provides all the required knowledge to carry on and pass the CISSP exam.