Information System Security Protection Knowledge and Preparation for Certification (CISSP)

Duration : 5 Days

Course Content

This course trains students in all areas of the security Common Body of Knowledge. They will learn security policy development, secure software development procedures, network vulnerabilities, attack types and corresponding countermeasures, cryptography concepts and their uses, disaster recovery plans and procedures, risk analysis, crucial laws and regulations, forensics basics, computer crime investigation procedures, physical security, and more

Prerequisites

Information System Knowledge

Course Objectives

After completing this course the student should be able to:

- Competently identify and handle security threats
- Gain credentials as a leading security professional for current and future employment
- Thoroughly understand the 8 essential core domains of the common body of knowledge

Who Should Attend

This course is designed for experienced security professionals who want to expand their knowledge and gain an internationally recognised accreditation. Whilst anyone can attend the course, please note that the CISSP accreditation is only available to those who meet the (ISC)2 entry requirements - see prerequisites below for more information.

Course Outline

- 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
- DOMAIN 6: Security Assessment and Testing
- DOMAIN 7: Security Operations
- DOMAIN 8: Software Development Security