

Certified Information Systems Security Professional (CISSP)

Course Description

This continuing education course provides instruction on preparing students for the Certified Information Systems Security Professional (CISSP) certification exam. Topics include security concepts, principles and methodologies

Course Objectives

Upon completion of this course, the students will be able to:

- Describe the principles of securing applications throughout the life cycle management process;
- Define the basic concepts within cryptography;
- Describe the access control concepts and methodologies;
- Identify the laws and legal issues that are applicable to computer crime'
- Perform business continuity planning.

Course Outline

- I. Information Security Management
 - A. Purposes of information security
 - B. Risk analysis and assessment
 - C. Information classification
 - D. Policies, procedures, standards and guidelines

- II. Security Architecture and Models
 - A. Information protection environment
 - B. Security technology and tools
 - C. Assurance, trust and confidence mechanisms

- III. Access Control Systems and Methodology
 - A. Information protection requirements
 - B. Centralized access control methodologies
 - C. Information protection and management
 - D. Intrusion detection

- IV. Operations Security
 - A. Cryptography
 - B. Physical security
 - C. Telecommunications, network and internet security
 - D. Business continuity planning

Training: 48 hours