



CISSP (Certified Information Systems Security Professional)

Course Duration: 5 days

Outline: **Lesson 1 - Information Security and Risk Management**

Information Security Management
Security Awareness Training and Education
Risk Management
Ethics

Lesson 2 - Access Control

Definitions and Key Concepts
Information Classification
Access Control Categories and Types
Access Control Threats
Access to Systems/Data
Access Control Technologies
Assurance Mechanisms

Lesson 3 - Cryptography

Key Concepts and Definitions
History
Encryption Systems
Symmetric and Asymmetric Algorithms
Message Integrity Controls
Digital Signatures
Management of Cryptographic Systems
Threats and Attacks

Lesson 4 - Physical Security

Definitions and Key Concepts
Site Location
Layered Defense Model
Infrastructure Support Systems
Equipment Protection

Lesson 5 - Security Architecture and Design

Components and Principles
System Security Techniques
Hardware
Software
Security Models and Architecture Theory
Security Evaluation Methods and Criteria

Lesson 6 - Business Continuity Planning and Disaster Recovery Planning

Project Scope Development and Planning

Business Impact Analysis
Emergency Assessment
Continuity and Recovery Strategy
Plan Design and Development
Implementation
Restoration
Plan Management

Lesson 7 - Telecommunications and Network Security

Key Concepts and Definitions
Networks
Protocols
Remote Access
Network Components
Telephony

Lesson 8 - Application Security

System Lifecycle Security
Application Environment and Security Controls
Programming Languages and Tools
Databases and Data Warehouses
Applications Systems Threats and Vulnerabilities
Applications Security Controls

Lesson 9 - Operations Security

Resource Protection
Change Control Management
Physical Security Controls
Privileged Entity Control

Lesson 10 - Legal, Regulations, Compliance and Investigation

Major Legal Systems
Legal Concepts
Regulatory Issues
Investigation
Computer Forensics