OVERVIEW

The Official CISSP training provides a comprehensive review of the knowledge required to effectively design, engineer and manage the overall security posture of an organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the CISSP exam.

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)

COURSE DURATION: 5 DAYS

COURSE OBJECTIVES

After completing this course, the student will be able to:

- Understand and apply fundamental concepts and methods related to the fields of information technology and security
- Align overall organizational operational goals with security functions and implementations
- Understand how to protect assets of the organization as they go through their lifecycle
- Understand the concepts, principles, structures and standards used to design, implement, monitor and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of confidentiality, integrity and availability
- Implement system security through the application of security design principles and application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures
- Understand the importance of cryptography and the security services it can provide in today's digital and information age
- Understand the impact of physical security elements on information system security and apply secure design principles to evaluate or recommend appropriate physical security protections
- Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function
- List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1-7
- Identify standard terms for applying physical and logical access controls to environments related to their security practice
- Appraise various access control models to meet business security requirements
- Name primary methods for designing and validating test and audit strategies that support business requirements
- Enhance and optimize an organization's operational function and capacity by applying and utilizing appropriate security controls and countermeasures
- Recognize risks to an organization's operational endeavors and assess specific threats, vulnerabilities and controls
- Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it; identify which security control(s) are appropriate for the development environment; and assess the effectiveness of software security.

TARGET STUDENT

The training seminar is ideal for those working in positions such as but not limited to:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect
- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Security Director
- Network Architect.

COURSE CONTENT

Lesson 1: Security and Risk Management

- Security Governance Principles
- Compliance
- Professional Ethics
- Security Documentation
- Risk Management
- Threat Modeling
- Business Continuity Plan Fundamentals
- Acquisition Strategy and Practice
- Personnel Security Policies
- Security Awareness and Training

Lesson 2: Asset Security

- Asset Classification
- Privacy Protection
- Asset Retention
- Data Security Controls

- Secure Data Handling

Lesson 3: Security Architecture and Engineering

- Security in the Engineering Lifecycle
- System Component Security
- Security Models
- Controls and Countermeasures in Enterprise Security
- Information System Security Capabilities
- Design and Architecture Vulnerability Mitigation
- Vulnerability Mitigation in Mobile, IoT, Embedded, and Web-Based Systems
- Cryptography Concepts
- Cryptography Techniques
- Site and Facility Design for Physical Security
- Physical Security Implementation in Sites and Facilities

Lesson 4: Communication and Network Security

- Network Protocol Security
- Network Components Security
- Communication Channel Security
- Network Attack Mitigation

Lesson 5: Identity and Access Management

- Physical and Logical Access Control
- Identification, Authentication, and Authorization
- Identity as a Service
- Authorization Mechanisms
- Access Control Attack Mitigation

Lesson 6: Security Assessment and Testing

- System Security Control Testing
- Software Security Control Testing
- Security Process Data Collection
- Audits

Lesson 7: Security Operations

- Security Operations Concepts
- Physical Security
- Personnel Security
- Logging and Monitoring
- Preventative Measures
- Resource Provisioning and Protection
- Patch and Vulnerability Management
- Change Management
- Incident Response
- Investigations
- Disaster Recovery Planning
- Disaster Recovery Strategies
- Disaster Recovery Implementation

Lesson 8: Software Development Security

- Security Principles in the System Lifecycle
- Security Principles in the Software Development Lifecycle
- Database Security in Software Development
- Security Controls in the Development Environment
- Software Security Effectiveness Assessment