



CERTIFIED

Information Systems Security Professional

Course Introduction:

In this course, participants will analyze a wide range of information systems security subjects that are organized into 8 domains for CISSP exam certification.

Course Objectives:

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

- Analyze information systems access control.
- Analyze security architecture and design.
- Analyze network security systems and telecommunications.
- Analyze information security management goals.
- Analyze information security classification and program development.
- Analyze risk management criteria and ethical codes of conduct.
- Analyze software development security.
- Analyze cryptography characteristics and elements.
- Analyze physical security.
- Analyze operations security.
- Apply Business Continuity and Disaster Recovery Plans.
- Identify legal issues, regulations, compliance standards, and investigation practices relating to information systems security.

Who Should Attend?

This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals, who are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current computer security careers or to migrate to a related career. Through the study of all 10 CISSP CBK domains, students will validate their knowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certification exam. The CISSP exam is intentionally difficult and should not be taken lightly. Even participants with years of security experience should assume that they will have additional study time after class. Because the domains are so varied, it is unlikely that any one student will have experience in all 10 domains.

Course Outline:

Security & Risk Management

- Security & Risk Management
- Confidentiality, Integrity, and Availability

- Security Governance
- The Complete and Effective Security Program
- Compliance
- Global Legal and Regulatory Issues
- Understand Professional Ethics
- Develop and Implement Security Policy
- Business Continuity (BC) & Disaster Recovery (DR) Requirements
- Manage Personnel Security
- Risk Management Concepts
- Threat Modeling
- Acquisitions Strategy and Practice
- Security Education, Training, and Awareness

Asset Security

- Asset Security
- Data Management: Determine and Maintain Ownership
- Data Standards
- Longevity and Use
- Classify Information and Supporting Assets
- Asset Management
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Standards Selection

Security Engineering

- Security Engineering
- The Engineering Lifecycle Using Security Design Principles
- Fundamental Concepts of Security Models
- Information Systems Security Evaluation Models
- Security Capabilities of Information Systems
- Vulnerabilities of Security Architectures
- Database Security
- Software and System Vulnerabilities and Threats
- Vulnerabilities in Mobile Systems
- Vulnerabilities in Embedded Devices and Cyber-Physical Systems
- The Application and Use of Cryptography
- Site and Facility Design Considerations
- Site Planning

- Implementation and Operation of Facilities Security

Communications & Network Security

- Communications & Network Security
- Secure Network Architecture and Design
- Implications of Multi-Layer Protocols
- Converged Protocols
- Securing Network Components
- Secure Communication Channels
- Network Attacks

Identity & Access Management

- Identity & Access Management
- Physical and Logical Access to Assets
- Identification and Authentication of People and Devices
- Identity Management Implementation
- Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Identity and Access Provisioning Lifecycle

Security Assessment & Testing

- Security Assessment & Testing
- Assessment and Test Strategies
- Collect Security Process Data
- Internal and Third-Party Audits

Security Operations

- Security Operations
- Investigations
- Provisioning of Resources through Configuration Management
- Resource Protection
- Incident Response
- Preventative Measures against Attacks
- Patch and Vulnerability Management
- Change and Configuration Management
- The Disaster Recovery Process
- Test Plan Review

- Business Continuity and Other Risk Areas
- Access Control
- Personnel Safety

Security in the Software Development Life Cycle

- Security in the Software Development Life Cycle
- Software Development Security Outline
- Environment and Security Controls
- Security of the Software Environment
- Software Protection Mechanisms
- Assess the Effectiveness of Software Security
- Assess Software Acquisition Security

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self-Questionnaires
- Group Work
- Discussion
- Presentation

Course Fees:

To be advice as per course location. This rate includes participant's manual, Hands-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session

