ISC2 Certified Information Systems Security Professional (CISSP) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The training certification is one of the most respected and globally recognized**Cyber Security Certifications** for experienced security professionals.

This official **ISC2 training course** provides a comprehensive review of the**ISC2 Common Body of Knowledge (CBK)** and prepares learners to design, implement, and manage enterprise-wide security programs.

Participants develop expertise across **Security and Risk Management**, **Asset Security**, **Security Architecture and Engineering**, **Network Security**, **Identity and Access Management (IAM)**, **Security Operations**, and **Software Development Security**.

Prerequisites

Learners should have:

- At least five years of cumulative paid experience in two or more CISSP domains
- Knowledge of **Information Security**
- Experience with **Risk Management**, **Network Security**, and **Access Control**

Who Should Attend

- Security Consultants
- Security Managers
- IT Directors
- Security Auditors
- Security Architects
- Security Analysts
- Security Engineers
- Chief Information Security Officers (CISO)
- Security Directors
- Network Architects

ISC2 Certified Information Systems Security Professional (CISSP) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this training, you will have gained knowledge and skills in the following areas:

- Apply core **Information Security** principles
- Align security strategies with business objectives
- Protect organisational assets throughout their lifecycle
- Design secure architectures and systems
- Apply **Cryptography** to secure communications and data
- Implement **Identity and Access Management (IAM)** solutions
- Conduct **Security Assessments** and **Security Testing**
- Manage **Security Operations** and incident response
- Reduce software and system security risks

Outline

1. Security and Risk Management

- Governance and Compliance
- CIA Triad
- Security Policies
- Ethics and Professional Responsibility
- Risk Management Frameworks

2. Asset Security

- Information Classification
- Data Ownership
- Data Lifecycle Management
- Data Protection Controls
- Compliance Requirements

3. Security Architecture and Engineering

- Secure Design Principles
- Security Models
- **Cryptography**
- Key Management
- Hardware Security
- System Security

4. Communication and Network Security

- Secure Network Design
- OSI Model
- Secure Communication Channels
- Wireless Security
- Remote Access Security
- SDN and Virtualization Security

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

5. Identity and Access Management (IAM)

- Identity Lifecycle Management
- Authentication
- Authorization
- Accountability
- Credential Management

6. Security Assessment and Testing

- Vulnerability Assessment
- Penetration Testing
- Security Audits
- Risk-Based Testing
- Security Evaluation

7. Security Operations

- Security Monitoring
- Incident Response
- Change Management
- Configuration Management
- Business Continuity
- Disaster Recovery

8. Software Development Security

- Secure Software Development
- Secure Coding Practices
- Application Security
- Database Security
- Vulnerability Management

9. Integrated Security Practices

- Digital Forensics
- Security Awareness Programs
- Supply Chain Security
- Third-Party Risk Management
- Enterprise Security Integration

CISSP is one of the most sought-after certifications for senior cyber security professionals and leadership roles worldwide.