Information Technology

Enterprise IT Security

Course Introduction

This training course is designed to provide participants with the fundamental knowledge necessary to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security.

Target Audience

IT managers, security analysts, network engineers, and cybersecurity professionals who want to gain expertise in securing enterprise IT infrastructures, focusing on developing and managing robust security measures, policies, and practices in large organizations.

Learning Objectives

- Proactively implement sound security protocols to mitigate security risks.
- Quickly respond to security issues.
- Retroactively identify where security breaches may have occurred.
- Design a network, on-site or in the cloud, with security in mind.

Course Outline

- **Day 01**

Day One

Security Fundamentals

- Security concepts
- Risk management
- Vulnerability assessment

Understanding attacks

- Understanding attackers

- ° Social engineering
- ° Malware
- ° Network attacks
- ° Application attacks

Cryptography

- ° Cryptography concepts
- ° Public key infrastructure

Network fundamentals

- ° Network components
- ° Network addressing
- ° Network ports and applications

• **Day 02**

Day Two

Securing networks

- ° Network security components
- ° Transport encryption
- ° Hardening networks
- ° Monitoring and detection

Securing hosts and data

- ° Securing hosts
- ° Securing data

- Mobile device security

Securing network services

- Securing applications
- Virtual and cloud systems

Authentication

- Authentication factors
- Authentication protocols

• **Day 03**

Access control

- Access control principles
- Account management

Organizational security

- Security policies
- User training
- Physical security and safety

Disaster planning and recovery

- Business continuity
- Fault tolerance and recovery
- Incident response

LABS

Understanding Attacks

- Examining Phishing Attacks
- Examining Malware
- Probing a Site
- Simulating a DOS Attack
- Cracking Passwords
- Simulating an Eavesdropping Attack
- Exploring Application Vulnerabilities
- Examining SQL Injection Attacks
- Examining Client-side Attacks

• **Day 04**

Day Four

Cryptography

- Symmetric Encryption
- Asymmetric Encryption
- Creating File Hashes
- Installing a Certificate Authority

Network Fundamentals

- Using TCP/IP Tools

Securing the Network

- Configuring a Firewall

- ° Examining Website Certificates
- ° Securing a WAP
- ° Viewing Event Logs
- ° Scanning the Network

Securing Hosts and Data

- ° Enabling BitLocker

• **Day 05**

Day Five

Securing Network Services

- ° Finding Vulnerable Code

Authentication

- ° Installing a RADIUS Server
- ° Examining Active Directory

Access Control

- ° Managing NTFS Permissions
- ° Managing Active Directory Objects
- ° Using Group Policy Objects
- ° Creating a Security Template

Disaster planning and recovery

- ° Using Windows Server Backup

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
April 7, 2025	April 11, 2025	5 days	4950.00 $	Norway - Oslo
Sept. 8, 2025	Sept. 12, 2025	5 days	4250.00 $	UAE - Dubai
Dec. 29, 2025	Jan. 2, 2026	5 days	4250.00 $	UAE - Dubai