**London TDM**

# Security Management and Risk Protection Training Courses

**Course Venue:** United Kingdom - London

**Course Date:** From 15 February 2026 To 19 February 2026

**Course Place:** London Paddington

**Course Fees:** 7,500 USD

## Introduction

In today's rapidly evolving digital landscape, ensuring secure access to systems and data is paramount for organizations. The "Access Control Systems and Protocols" course provides a comprehensive understanding of how to implement and manage access control frameworks effectively. Throughout this five-day program, participants will engage in insightful discussions, practical exercises, and in-depth case studies to enhance their skills in safeguarding information assets.

## Objectives

- Understand the fundamentals of access control systems and their importance in cybersecurity.
- Explore different types of access control methods and protocols.
- Learn how to implement access control policies and mechanisms effectively.
- Identify potential vulnerabilities and threats related to access control.
- Gain practical experience in deploying and managing access control systems.

## Course Outlines

### Day 1: Introduction to Access Control Systems

- Overview of Access Control Concepts
- Importance of Access Control in Information Security
- Types of Access Control: Discretionary, Mandatory, Role-Based
- Access Control Models: Bell-LaPadula, Biba, Clark-Wilson
- Challenges and Trends in Access Control

### Day 2: Authentication Protocols and Technologies

- Basics of Authentication and Authorization
- Password-Based Authentication: Best Practices and Limitations
- Multi-Factor Authentication: Implementation Strategies
- Biometric Authentication: Applications and Concerns
- Public Key Infrastructure (PKI) and Certificate-Based Authentication

### Day 3: Designing and Implementing Access Control Policies

- Defining Access Control Policies and Procedures
- Access Control Lists (ACLs) and Capabilities
- Implementing Role-Based Access Control (RBAC)
- Access Control in Cloud Environments
- Monitoring and Auditing Access Control Systems

### Day 4: Vulnerabilities and Threats in Access Control

- Common Vulnerabilities in Access Control Systems
- Case Studies: Analyzing Security Breaches
- Mitigating Unauthorized Access and Insider Threats
- Encryption and Access Control: Synergies and Conflicts
- Incident Response and Recovery Planning

**Day 5: Practical Application and Case Studies**

- Hands-On Lab: Setting Up Access Control Mechanisms
- Simulating Access Control Breaches and Responses
- Review and Analysis of Real-World Access Control Failures
- Group Project: Designing a Comprehensive Access Control System
- Course Review and Final Assessment