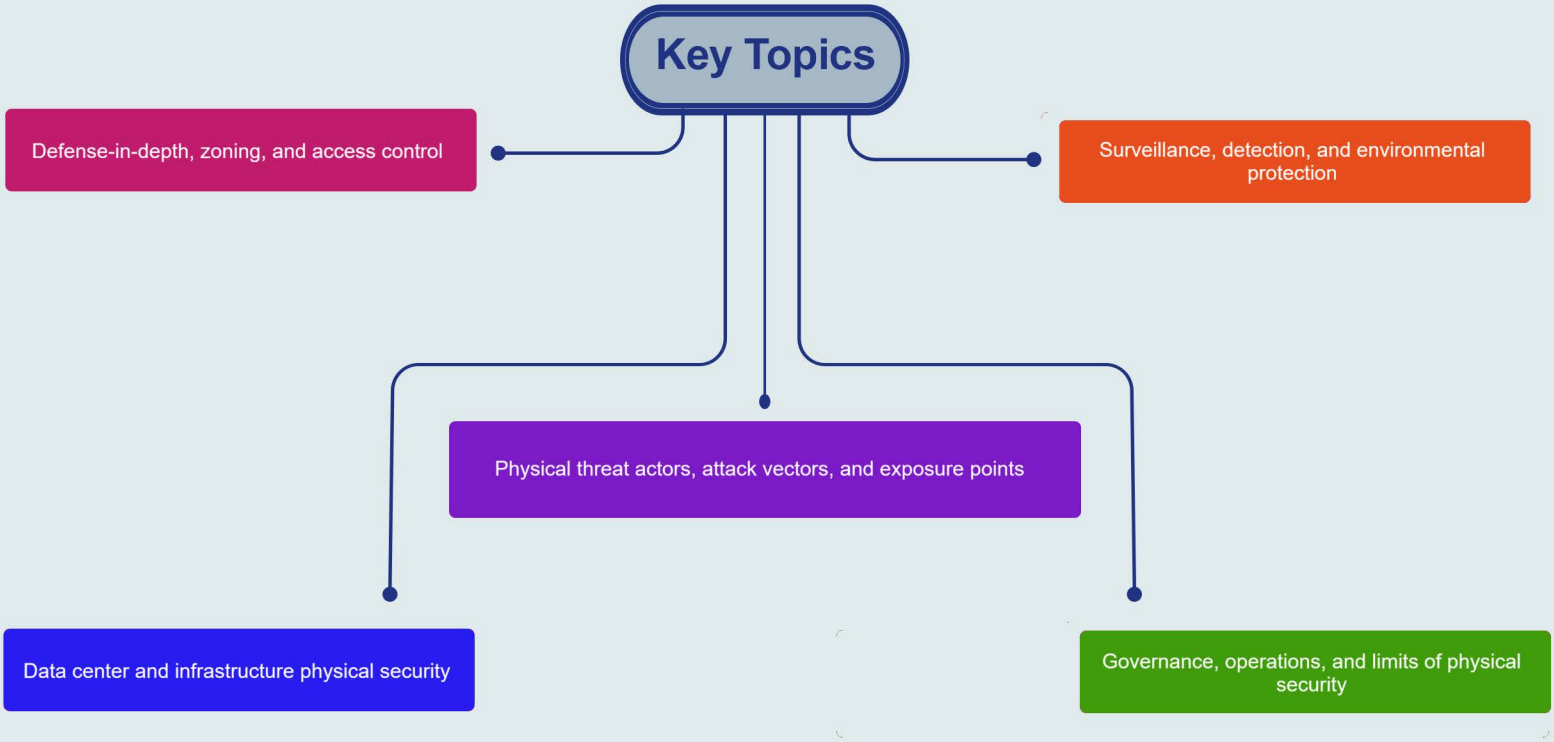
About the Course

This course provides a structured and risk-driven understanding of physical security as a foundational trust anchor for information security, operational resilience, and business continuity. It explains why physical security remains critical even in highly digital and cloud-centric environments, and how failures at the physical layer can completely undermine logical, network, and data controls. The course examines physical threat actors, attack vectors, exposure points, and indicators of compromise from a security and governance perspective. It covers defense-in-depth, zoning, access control, surveillance, environmental protection, and resilience controls across facilities, data centers, and supporting infrastructure. Emphasis is placed on integration with ISMS, incident response, and compliance obligations. The course positions physical security as a governance, risk, and operational discipline—not merely guards and cameras.

Learning Objectives

1. A clear understanding of physical security as a trust anchor
2. The ability to identify physical attack surfaces and threat vectors
3. A structured understanding of defense-in-depth for physical environments
4. The ability to design security zoning and access control strategies
5. A conceptual understanding of monitoring, response, and resilience controls
6. The ability to integrate physical security into ISMS and compliance programs

Key Topics



Pre Requisites

- Basic understanding of information security principles and governance, compliance, or operational security concepts
    - Information Security Essential Courses
- General knowledge of IT infrastructure or organizational operations

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files & Toolkit
- Information Security Tactics eBook

Who Should Attend

- Physical security and facilities security managers
- Information Security and ISMS Managers
- Infrastructure, data center, and operations leaders
- Security architects and enterprise architects
- Business continuity and resilience professionals
- Professionals preparing for ISO/IEC 27001, CISM, or CISSP roles

Syllabus

Foundations of Physical Security

- Purpose and role of physical security
- Physical security as a trust anchor
- Relationship to information security, networks, data, and BCDR

Threat Actors, Attack Vectors, and Exposure Points

- Criminals, insiders, activists, and espionage
- Tailgating, impersonation, sabotage, and environmental attacks
- Perimeters, entrances, server rooms, and shared spaces

Indicators of Compromise and Defense-in-Depth

- Signs of forced entry and tampering
- Detection, delay, response, and recovery
- Layered physical protection models

Zoning, Perimeter, and Access Controls

- Public, controlled, restricted, and high-security zones
- Fencing, lighting, barriers, and entry systems
- Badges, biometrics, mantraps, and visitor management

Monitoring, Surveillance, and Alarms

- CCTV placement and blind spots
- Motion, door, glass-break, and environmental sensors
- Monitoring procedures and privacy considerations

Critical Infrastructure and Environmental Protection

- Data centers, server rooms, and wiring closets
- Media, archives, and backup storage
- Fire, water, power, HVAC, and utility resilience

Syllabus

Operations, Policies, and Compliance

- Access reviews, patrols, and physical incident handling
- Physical security policies and procedures
- ISO 27001, SOC, PCI, and audit readiness

Testing, Common Failures, and Limits

- Walkthroughs, red-team testing, and social engineering
- Common physical security failures
- Limits of physical security and governance dependencies

Hands-on Training

- Physical Security Risk and Attack Surface Assessment
- Security Zoning and Defense-in-Depth Design
- Physical Access Control Strategy Implementation
- Surveillance and Monitoring Strategy Design
- Environmental and Infrastructure Protection Planning
- Physical Security Governance and Incident Response Integration