About the Course

This foundational course provides a conceptual, managerial, and strategic understanding of Information Security as a business and organizational discipline. It is designed for learners who have general IT knowledge but need a proper mental model of security before diving into technical domains.

The course covers:

- The essence, philosophy, and evolution of information security
- The core conceptual model: Asset, Threat, Vulnerability, Risk, Control
- The fundamental security objectives (CIA, trust, access control, GRC, resilience)
- The Information Security Management System (ISMS) and its organizational role
- A structured overview of global security guidance and frameworks (NIST, ISO, CIS, etc.)

This course forms the intellectual foundation and prerequisite for all advanced courses in cybersecurity, governance, risk, compliance, architecture, operations, and auditing.

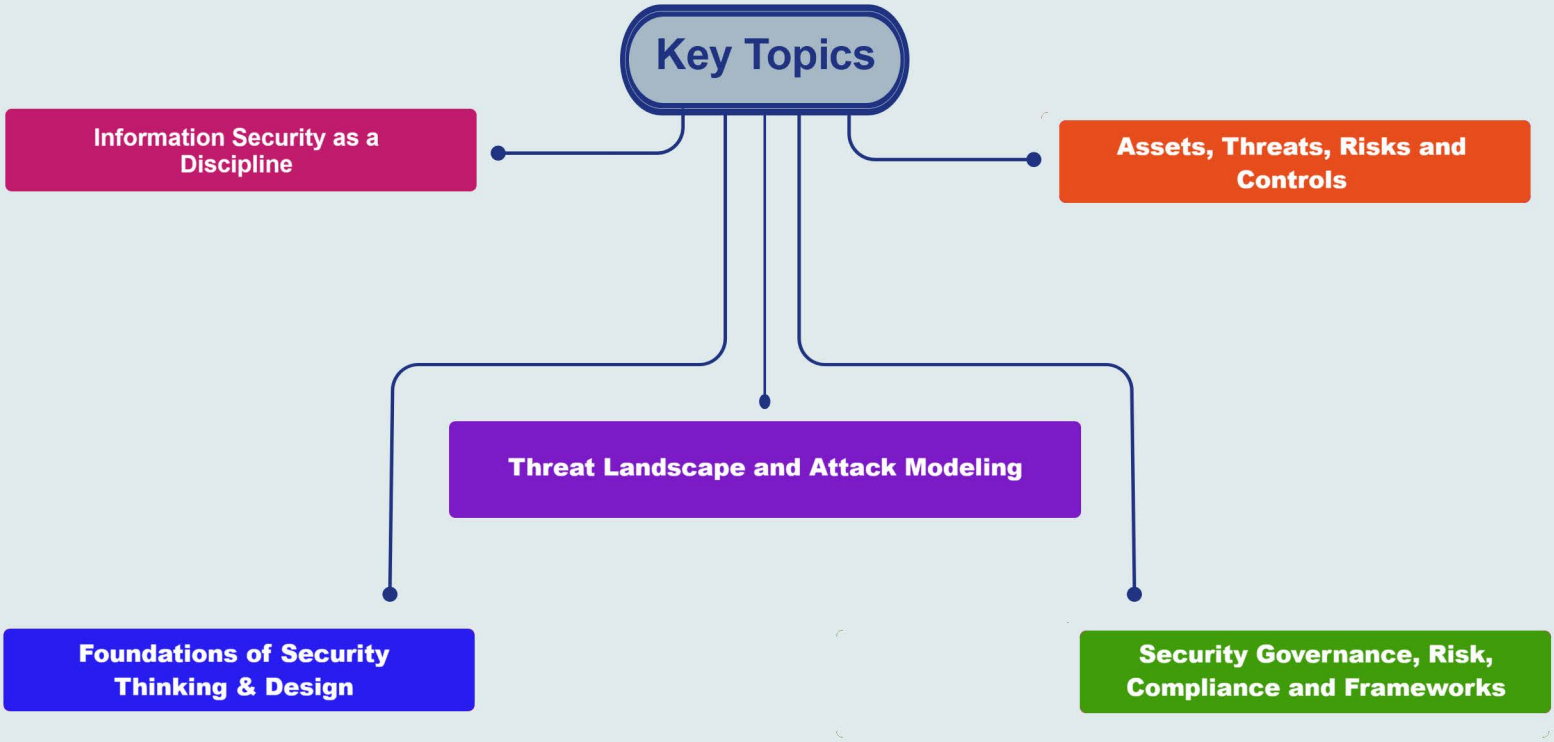
Learning Objectives

1. A **deep conceptual understanding of Information Security**
2. A **clear mental model of Asset–Threat–Vulnerability–Risk–Control**
3. A **practical understanding of CIA, trust, access control, GRC, and resilience**
4. A **map of the global security standards, frameworks, and guidance ecosystem**
5. A **solid understanding of security principles and design philosophy**
6. A **managerial understanding of ISMS and ISO/IEC 27001**

Information Security Fundamentals

Terminus System

Key Topics



Pre Requisites

- Basic knowledge of:
  - Networking concepts
  - IT systems
- No prior security knowledge required

Information Security Fundamentals

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Mastering Information Security – Understanding Fundamentals eBook

Who Should Attend

- Future **Information Security Managers and Architects**
- **Cybersecurity professionals** who want conceptual mastery
- **Risk, compliance, audit, and governance** professionals
- **IT managers and decision makers**
- Students preparing for **Security+, CISSP, CISM, ISO 27001**, and similar tracks
- Anyone who wants to **understand security as a system, not as tool**.

Syllabus

The Essence of Information Security

- Why information security matters
- What information security is
- History and evolution
- Cybersecurity vs information security
- Changing threat landscape
- Core security principles and secure design philosophy

Core Conceptual Model of Information Security

- Assets, vulnerabilities, threats, attacks, and threat vectors
- Risk as a function of asset, threat, and vulnerability
- Security controls: categories, types, and layers
- The Asset–Threat–Vulnerability–Risk–Control relationship model
- Systemic view of information security

Core Security Concepts

- CIA Triad: Confidentiality, Integrity, Availability
- Authenticity, non-repudiation, and digital trust
- Access control and the AAA model
- Governance, Risk, and Compliance (GRC)
- Organizational resilience and continuity

Information Security Management

- Information Security Management System (ISMS)
- Strategic, tactical, and operational management levels
- Integration of ISMS, GRC, and resilience
- Overview of ISO/IEC 27001

Information Security Guidance & Standards

- NIST SP 800 series guidance
- ISO/IEC 27000 family
- CIS and OWASP guidance
- Sector and domain guidance (e.g., PCI, ICS, critical infrastructure)

Syllabus

Measurement, Assessment, and Governance

- Security measurement and performance indicators
- Security posture and capability assessment
- Maturity models and management dashboards

Implementation Approaches and Methodologies

- Control-based, risk-based, process-based, and governance-driven approaches
- Frameworks, standards, and methodologies positioning
- Security lifecycle and multi-year transformation programs

Applied Exercises

- Case-based exercises
- Scenario-based analysis
- MCQs and knowledge checks