Data Security

Terminus System

About the Course

There is a simple principle in information security: protect your most valuable asset—data—while maximizing business value.
You should consider all forms of data—digital, physical, and human knowledge—and address their full lifecycle:

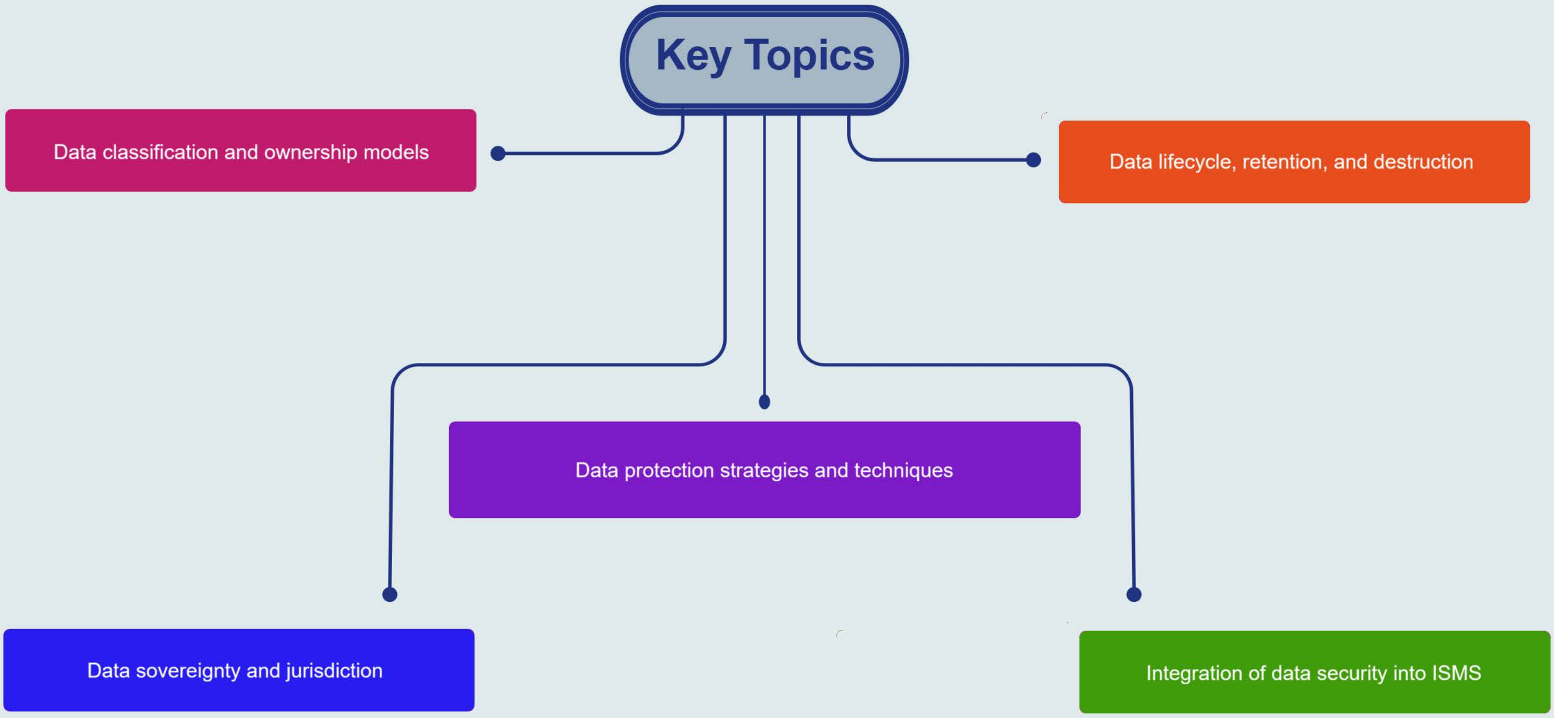
- At Rest: Stored on devices, servers, or cloud
- In Transit: Moving across networks, applications, or cloud services
- In Process: Actively used in systems, applications, or cloud compute

This course provides a structured and governance-oriented understanding of data security as a core pillar of information security rather than a purely technical function. It examines data as a strategic organizational asset and explains how data must be classified, governed, protected, retained, and destroyed across its entire lifecycle. The course focuses on roles, responsibilities, regulatory drivers, data states, sovereignty, and lifecycle-based protection strategies within ISMS and GRC frameworks. It emphasizes policy-driven, standards-based, and legally defensible approaches to protecting data across on-premises, cloud, and hybrid environments.

Learning Objectives

1. A governance-oriented understanding of data security
2. The ability to classify organizational data based on impact and sensitivity
3. A clear understanding of data roles, responsibilities, and accountability
4. A lifecycle-based view of data handling, retention, and destruction
5. Awareness of data sovereignty, jurisdiction, and regulatory constraints
6. The ability to integrate data security into ISMS and GRC structures

Key Topics



Key Topics

Data classification and ownership models

Data lifecycle, retention, and destruction

Data protection strategies and techniques

Data sovereignty and jurisdiction

Integration of data security into ISMS

Pre Requisites

- **Information Security Fundamentals**
- **Information Security Standards, Frameworks, and Best Practices**
- **Information Security Risk Management**

Data Security

Terminus
System

What You Will Receive

Course Presentation File

Complementary Files & Toolkit

Information Security Tactics eBook

Who Should Attend

- Information Security Managers and ISMS Managers
- GRC, risk, compliance, and audit professionals
- Data protection and privacy specialists
- Security architects and enterprise architects
- IT managers and system owners responsible for data
- Professionals preparing for ISO/IEC 27001, ISO 27701, CISM, or CISSP

Syllabus

Foundations of Data Security and Governance

- Data as a strategic organizational asset
- Role of data security in information security, ISMS, and GRC
- Relationship between data protection, governance, risk, and compliance

Types of Data and Regulatory Context

- Regulated and non-regulated data
- PII, PHI, financial, legal, IP, biometric, and government data
- High-level regulatory and compliance drivers

Data Classification and Accountability Models

- Purpose and value of data classification
- Impact-based and organizational classification models
- Data roles, responsibilities, and RACI accountability

Data States, Location, and Sovereignty

- Data at rest, in transit, and in use
- On-premises, cloud, and hybrid data locations
- Jurisdiction, residency, and cross-border constraints

The Data Lifecycle and Operational Handling

- Data creation and lawful collection
- Data usage, maintenance, and storage
- Retention and defensible destruction

Data Quality, Integrity, and Retention

- Accuracy, consistency, and integrity requirements
- Backups, versioning, and operational responsibilities
- Retention schedules and auditability

Syllabus

Data Protection Strategy and Techniques

- Defense-in-depth for data
- Administrative, technical, and physical controls
- Standards-based data protection techniques

Integrating Data Security into ISMS

- Mapping data security to policies and standards
- Risk management linkage
- Governance, monitoring, and continuous improvement

Hands-on Training

- Organizational Data Classification Framework Design
- Data Lifecycle and Retention Strategy
- Data Sovereignty and Cross-Border Risk Assessment
- Integrating Data Security into ISMS Governance