About the Course

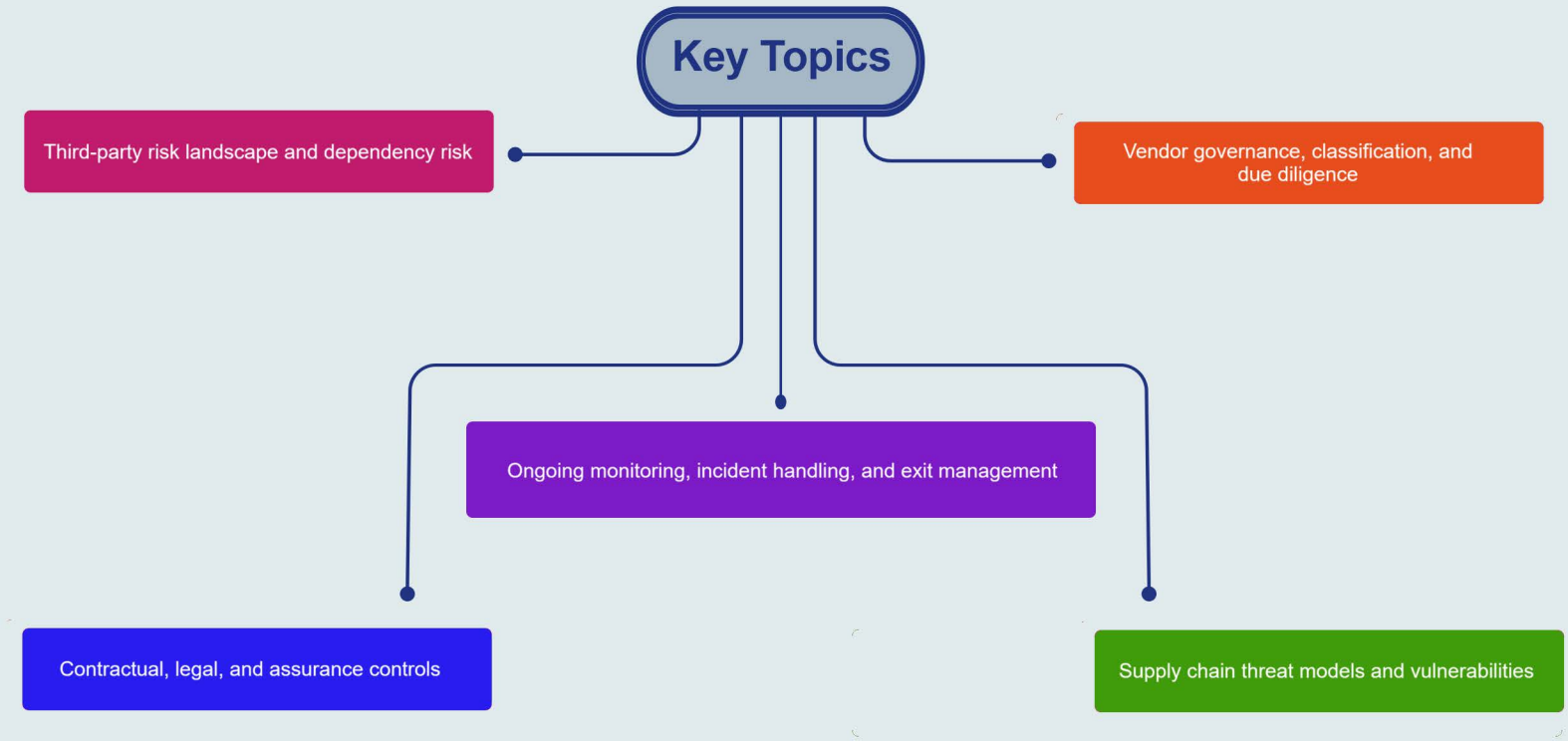
This course provides a structured and governance-driven understanding of third-party and supply chain security as a first-class risk domain in modern organizations. It explains why no organization operates in isolation and how dependencies on vendors, service providers, software suppliers, and partners expand the attack surface beyond organizational boundaries. The course examines third-party risk landscapes, governance models, classification approaches, and assurance mechanisms.

It covers due diligence, contractual controls, onboarding, monitoring, incident coordination, and exit management. Emphasis is placed on dependency risk, concentration risk, and systemic risk across complex supply chains. The course positions third-party and supply chain security as a governance, risk, and architectural discipline tightly integrated with ISMS, compliance, and enterprise risk management.

Learning Objectives

1. A clear understanding of third-party and supply chain security as a core risk domain
2. The ability to identify and classify third-party and dependency risks
3. A structured understanding of vendor governance, ownership, and accountability
4. The ability to apply due diligence and assurance mechanisms
5. A conceptual understanding of supply chain threat models and vulnerabilities
6. The ability to integrate third-party risk into ISMS and governance frameworks

Key Topics



Pre Requisites

- Basic understanding of information security and risk management principles
  - Information Security Essentials Courses
- General knowledge of organizational operations or IT services sourcing
- Familiarity with compliance, governance, or procurement processes
  - Information Security Risk Management Course

Terminus System

What You Will Receive

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

Who Should Attend

- Information Security and ISMS Managers
- GRC, risk, and compliance professionals
- Procurement, vendor management, and legal teams
- Security architects and enterprise architects
- IT and business owners of third-party services
- Professionals preparing for CISSP, CISM, or ISO/IEC 27001 roles

Syllabus

Foundations of Third-Party and Supply Chain Security

- Purpose and role of third-party risk management
- Dependency risk as a first-class security concern
- Relationship to risk management, governance, compliance, and architecture

Third-Party Risk Landscape and Classification

- Types of third parties and service relationships
- Direct vs indirect (fourth-party) risk
- Criticality, data access, network access, and dependency levels

Governance, Ownership, and Vendor Selection

- Business vs risk ownership
- Roles of procurement, legal, security, and business
- Vendor selection, due diligence, and conflict management

Risk Assessment, Assurance, and Contracts

- Risk assessment methods and evidence collection
- Certifications, audits, and independent assurance
- Contractual controls, security clauses, and audit rights

Vendor Onboarding and Secure Integration

- Access provisioning and segmentation
- Data access scoping and monitoring enablement
- Integration risks and control alignment

Ongoing Monitoring and Oversight

- Periodic reassessments and continuous monitoring
- Evidence refresh and KPI/KRI tracking
- Managing concentration and systemic risk

Syllabus

Supply Chain Threats and Incident Handling

- Software, hardware, and service supply chain attacks
- Shared incident response and coordination
- Evidence access and legal constraints

Exit Management, Common Failures, and Limits

- Termination, offboarding, and residual risk handling
- Common third-party security failures
- Limits of third-party risk management and dependency design

Hands-on Training

- Third-Party Risk Landscape and Dependency Mapping
- Vendor Classification and Risk Tiering Model Design
- Third-Party Due Diligence and Assurance Assessment
- Contractual Security Controls and Governance Requirements
- Third-Party Integration and Ongoing Monitoring Model
- Supply Chain Incident Response and Exit Management Planning