CONCEPT

Third-Party Risk Management (TPRM) and Outsourcing Risk Governance

Third-Party Risk Management (TPRM) and Outsourcing Risk Governance

Technical depth: Practitioner · **Practical mode:** Case study

Introduction

Organisations now depend on cloud providers, outsourcers, suppliers and their subcontractors for services they once ran themselves, yet many cannot list their critical third parties, let alone the fourth parties behind them. Due diligence is a one-off questionnaire, contracts lack audit and exit rights, and a single provider outage can stop core operations. This Core Concept course equips managers to govern third-party and outsourcing risk across the full relationship lifecycle. Participants work on cases from several sectors and leave with a Third-Party Risk Governance Framework for their own organisation.

Course Objectives

- Build a third-party inventory and classify providers by criticality, risk category and nth-party dependency
- Apply international third-party risk principles and supplier security standards to design a risk governance framework
- Conduct risk-based due diligence, including review of independent assurance reports, before contracting
- Negotiate the contractual protections, service levels and monitoring arrangements that critical services require
- Assess concentration, cloud and fourth-party risk, and prepare exit and continuity plans for critical services
- Produce a Third-Party Risk Governance Framework ready for management approval

Target Audience

- Procurement, sourcing and vendor managers selecting and contracting providers
- Risk and compliance managers responsible for third-party and outsourcing risk
- Contract and relationship managers overseeing service levels and performance
- Information security and IT managers assessing cloud and technology providers
- Business continuity and operational resilience managers planning for provider failure
- Internal audit managers reviewing third-party risk management

Course Outline

Day 1: The Third-Party Landscape and Criticality

- Third-Party Ecosystem Mapping: Suppliers, Outsourcers, Cloud Providers and Nth Parties
- Material Outsourcing and Critical Service Classification Criteria
- Third-Party Inventory and Criticality Tiering Model
- Third-Party Risk Taxonomy: Operational, Cyber, Financial, Compliance and Reputational
- Third-Party Risk Programme Maturity Assessment Across Lifecycle Stages

Day 2: Third-Party Risk Frameworks and Standards

- Basel Committee Principles for the Sound Management of Third-Party Risk 2025
- ISO/IEC 27036-2:2022 Supplier Relationship Security Requirements
- ISO 22318:2021 Supply Chain Continuity Guidelines
- ISO 37001:2025 Due Diligence on Business Associates
- Third-Party Risk Policy and Governance Roles Under the Three Lines Model

Day 3: Managing the Third-Party Lifecycle

- Risk-Based Due Diligence Using the SIG Questionnaire
- Independent Assurance Review: ISAE 3402 and SOC 2 Reports
- Outsourcing Contract Clauses: Audit Rights, Subcontracting and Termination
- Service Level Agreements and Third-Party Performance Scorecards
- Ongoing Monitoring and Periodic Reassessment Calendar

Day 4: Concentration, Cloud and Exit Risk

- Concentration Risk and Single Point of Failure Analysis
- Fourth-Party and Subcontractor Dependency Mapping
- Cloud Provider Assessment Using the CSA Cloud Controls Matrix
- Exit Strategy and Continuity Plans for Critical Services Under ISO 22301:2019
- Third-Party Incident Escalation and Issue Management Workflow

Day 5: Case Work and the Governance Framework

- Cloud Outage Case Study: Critical Service Disruption Response
- Logistics Outsourcing Case Study: Due Diligence Failure Review
- Criticality Tiering Exercise for an Own Supplier Portfolio
- Third-Party Risk Governance Framework Drafting
- Peer Review Panel and Framework Defence

Skills You Will Gain

- Third-Party Criticality Assessment
- Risk-Based Due Diligence
- Assurance Report Evaluation
- Outsourcing Contract Risk Review
- Supplier Performance Monitoring
- Concentration Risk Analysis
- Exit Planning
- Third-Party Incident Management

Why Attend This Course

- Return to work with a Third-Party Risk Governance Framework for your own organisation, already tested by peers
- Know which of your providers are critical, which fourth parties sit behind them and what happens if one fails
- Read an assurance report or a contract and spot the gaps that leave the organisation exposed
- Compare third-party practice with managers from other sectors and countries who rely on similar providers

Conclusion

Outsourcing transfers the work, never the accountability, and a provider's failure quickly becomes the organisation's own. This course moves from mapping and tiering the third-party ecosystem, through international principles and supplier security and continuity standards, to due diligence, contracting, monitoring and the concentration, cloud and exit risks that cause the largest disruptions. The final day turns that material into a Third-Party Risk Governance Framework that participants take back to management, giving them a structured and defensible basis for every provider relationship.