IT Governance and Third-Party Cyber Risk Oversight: COBIT 2019 and ISO/IEC 38500

IT Governance and Third-Party Cyber Risk Oversight: COBIT 2019 and ISO/IEC 38500

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

Introduction

Most organisations now depend on cloud platforms, managed service providers and software suppliers for services they once ran themselves, so a single supplier breach or outage can halt operations across the business. Boards and executive teams remain accountable for that exposure, yet IT decisions and supplier assurance often sit in separate silos with no common risk view. This Core Concept course equips executives to direct IT governance and oversee third-party cyber risk using ISO/IEC 38500, COBIT 2019 and NIST CSF 2.0. Participants leave with a Third-Party Cyber Risk Governance Framework for their organisation.

Course Objectives

- Define board and executive decision rights for technology using ISO/IEC 38500:2024 and COBIT 2019 governance objectives
- Set a technology and cyber risk appetite that guides investment, sourcing and supplier decisions
- Oversee supplier criticality tiering, due diligence and contractual protections against NIST CSF 2.0 supply chain outcomes
- Challenge assurance evidence such as SOC 2 reports, ISO/IEC 27001 certificates and security questionnaires
- Evaluate concentration, fourth-party and exit risk in cloud and outsourced services and direct mitigation
- Produce a Third-Party Cyber Risk Governance Framework ready for board or executive committee approval

Target Audience

- Executives accountable for technology strategy, digital investment and IT operations
- Executives overseeing information security and enterprise cyber risk
- Heads of procurement and vendor management responsible for critical technology suppliers
- Heads of risk, compliance and internal audit who provide assurance on technology risk
- Board and committee members with oversight of technology, cyber and outsourcing risk
- Business unit heads whose operations rely on outsourced or cloud-based digital services

Course Outline

Day 1: The IT Governance and Digital Dependency Landscape

- IT Governance Versus IT Management under ISO/IEC 38500:2024
- Governing Body Accountability under ISO 37000:2021 Principles
- Digital Supply Chain Dependency and Concentration Risk Map
- Lessons from Major Supply Chain Incidents: SolarWinds, MOVEit and the 2024 CrowdStrike Outage
- IT Governance Current-State Review Using COBIT 2019 Capability Levels

Day 2: Governance and Supplier Security Frameworks

- COBIT 2019 Governance System, Design Factors and Focus Areas
- COBIT 2019 EDM Objectives: Evaluate, Direct and Monitor
- NIST CSF 2.0 Govern Function and GV.SC Supply Chain Outcomes
- ISO/IEC 27036 Series for Supplier Relationship Security
- ISO/IEC 27001:2022 Annex A Supplier Controls 5.19 to 5.23

Day 3: Directing Technology Decisions and Supplier Oversight

- Technology Risk Appetite Statement and Tolerance Thresholds
- Third-Party Inventory and Criticality Tiering Model
- Assurance Evidence Review: SOC 2 Type II Reports, ISO/IEC 27001 Certificates and the SIG Questionnaire
- Cyber Contract Clauses: Right to Audit, Breach Notification and Exit Terms
- IT Investment Portfolio Oversight Using COBIT APO05

Day 4: Advanced Third-Party Risk and Resilience

- Fourth-Party and Nth-Party Risk Mapping
- Cloud Shared Responsibility and the CSA Cloud Controls Matrix v4
- Software Supply Chain Assurance with SBOM and NIST SP 800-161 Rev. 1
- Continuous Supplier Monitoring with Security Ratings and Key Risk Indicators
- Supplier Exit and Substitutability Planning Aligned to ISO 22301:2019

Day 5: Case Work and the Governance Framework

- Critical Cloud Provider Outage Case Study: Board Oversight Gaps
- Managed Service Provider Breach Case Study: Contract and Assurance Failures
- Board Technology and Third-Party Risk Dashboard Design
- Third-Party Cyber Risk Governance Framework Drafting
- Executive Committee Review and Framework Defence

Skills You Will Gain

- Technology Decision Rights Design
- Cyber Risk Appetite Setting
- Supplier Criticality Assessment
- Assurance Evidence Evaluation
- Concentration Risk Oversight
- Technology Contract Governance
- Board Risk Reporting

Why Attend This Course

- Return to work with a Third-Party Cyber Risk Governance Framework for your organisation, already challenged by peer executives
- Ask suppliers and internal teams the questions that reveal whether assurance is real or only on paper
- Recognise dangerous dependence on a single cloud or service provider before an outage exposes it
- Compare governance practice with executives from other sectors and countries who rely on the same global suppliers

Conclusion

Outsourcing a technology service does not outsource accountability for the risk it carries. This course moves from the principles of IT governance and the scale of digital dependency, through COBIT 2019, ISO/IEC 38500 and NIST CSF 2.0, to supplier tiering, assurance evidence, contract protections and concentration risk. The final day turns that material into a Third-Party Cyber Risk Governance Framework that participants take back to their board or executive committee, giving them a clear and defensible basis for overseeing the suppliers their organisation depends on.