IT Risk Management and Cybersecurity Training Course for Organisations

22 – 26 March 2027
San Diego

AGILE LEADERS
Training Center

IT Risk Management and Cybersecurity Training Course for Organisations

Ref: 36392_97708 **Date:** 22 – 26 March 2027 **Location:** San Diego **Fees:** 14000 Euro

Overview

IT risk management at organisation level is about deciding how much technology and cyber risk the business is willing to carry, who owns it, and how the board sees it. This course treats IT and cybersecurity risk as a portfolio across the whole enterprise rather than one application at a time. Participants connect ISO 31000 principles, COBIT governance objectives and the NIST Cybersecurity Framework 2.0 into one operating model: setting risk appetite and tolerances, running an enterprise IT risk register, aligning controls with business objectives, planning continuity and recovery, and reporting cyber exposure in language executives act on. The final days look ahead to cloud, IoT, artificial intelligence and ransomware. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- IT directors, CIOs and heads of infrastructure
- CISOs and cybersecurity programme managers
- Enterprise risk and GRC professionals covering technology risk
- Business continuity and resilience coordinators
- Internal auditors and compliance managers reviewing IT governance

Departments and Industries

Relevant wherever technology and cyber risk must be governed and reported across the whole organisation.

- Governance, risk and compliance offices
- Cybersecurity and IT operations
- Business continuity and crisis management units
- Banking, insurance and financial services
- Energy, government, healthcare, retail and e-commerce

Learning Objectives

By the end of this course, participants will be able to:

- Apply ISO 31000, COBIT and the NIST Cybersecurity Framework together in one enterprise IT risk process.
- Define IT and cyber risk appetite, tolerance levels and ownership across business units.
- Evaluate the enterprise technology risk portfolio using heat maps, scenarios and key risk indicators.
- Develop treatment strategies that combine preventive, detective and corrective controls with business continuity plans.
- Prepare board-level IT risk reports and dashboards that support investment decisions.
- Assess emerging risks from cloud services, IoT, artificial intelligence and ransomware.

Course Agenda

Day 1: Foundations of Enterprise IT Risk

- Types and sources of technology and cyber risk and their business impact
- Risk appetite, tolerance and residual risk at organisation level
- ISO 31000 principles, framework and process
- Positioning IT risk inside enterprise risk management
- Regulatory and compliance expectations for technology risk

Day 2: Frameworks and Governance Structures

- COBIT governance and management objectives for risk
- The six functions of the NIST Cybersecurity Framework 2.0
- Mapping frameworks to a single control set
- Three lines model, committees and risk ownership
- Policies and standards that turn appetite into rules

Day 3: Enterprise Risk Analysis and Treatment

- Building and maintaining an enterprise IT risk register
- Scenario analysis and heat maps across business units
- Treatment options and aligning them with business objectives
- Preventive, detective and corrective control portfolios
- Third-party and supply chain technology risk

Day 4: Resilience, Monitoring and Board Reporting

- Business continuity and IT disaster recovery planning
- Incident response readiness and crisis communication
- Key risk indicators and continuous risk monitoring
- Designing dashboards for executives and the board
- Linking risk reports to budgets and investment decisions

Day 5: Emerging Technology Risks

- Cloud and hybrid environments: shared responsibility and concentration risk
- IoT and operational technology exposure
- Artificial intelligence and machine learning risks
- Ransomware preparedness, recovery and cyber insurance
- Building a roadmap to mature the IT risk programme

Practical Exercises

Working in teams on a fictional mid-sized company, participants complete these suggested activities.

- Suggested activity: draft an IT and cyber risk appetite statement with tolerances for three business units.
- Suggested activity: map the company's current controls to COBIT objectives and the NIST Cybersecurity Framework functions.
- Suggested activity: run a ransomware scenario workshop and test the continuity and recovery plan against it.
- Suggested activity: build a one-page board risk report with key risk indicators and a treatment roadmap.

FAQs

How is this different from a risk assessment of a single IT system?

This course works at enterprise level: appetite, governance, portfolio, continuity and board reporting. It does not walk one system through a technical assessment.

Do I need a technical security background?

No. Familiarity with IT operations or risk concepts helps, but the content is aimed at managers and governance roles.

Which frameworks are covered?

ISO 31000, COBIT and the NIST Cybersecurity Framework, used together rather than one at a time.

Conclusion

Participants leave with a practical model for IT risk management across the organisation: a clear appetite, shared frameworks, a living risk register, tested continuity plans and reports the board can act on, ready to strengthen cybersecurity governance in their own organisation.