Telecom Risk and Regulatory Compliance Essentials

7 – 11 December 2026
Lisbon

AGILE LEADERS
Training Center

Telecom Risk and Regulatory Compliance Essentials

Ref: **103600635_108297** **Date:** **7 – 11 December 2026** **Location:** **Lisbon** **Fees:** **5700 Euro**

Course Overview:

The Telecom Risk and Regulatory Compliance Training Course equips participants to manage regulatory, operational, cybersecurity, privacy, fraud, competition, and continuity risks across telecommunications organizations.

The course explains the Telecom Regulatory Framework governing licensing, spectrum, interconnection, competition, consumer protection, privacy, and network security. It also shows how sector regulation interacts with competition law and why operators must maintain effective compliance programmes.

Using ITU-T X.1055 and NIST risk-management guidance, participants learn how to conduct Telecom Risk Assessment, classify risks, select controls, assign risk ownership, prioritize treatment actions, and report exposure to management.

The course combines Telecom Risk Management with practical Telecom Compliance Training, helping participants improve Telecom Governance and Compliance, Telecom Cybersecurity Compliance, Telecom Data Privacy Compliance, Telecom Audit and Compliance, Telecom Fraud Risk Management, Telecom Network Security, and Telecom Business Continuity.

Target Audience:

- Telecom Risk and Compliance Managers
- Regulatory Affairs and Legal Professionals
- Internal Auditors and GRC Specialists
- Cybersecurity and Network Security Managers
- Data Protection and Privacy Officers
- Fraud and Revenue Assurance Professionals
- Business Continuity Managers
- Telecom Operations and Engineering Managers
- Licensing, Spectrum, and Interconnection Specialists
- Senior Managers responsible for telecom governance

AGILE LEADERS
Training Center

Targeted Organizational Departments:

- Regulatory Affairs and Licensing
- Enterprise Risk Management
- Legal and Compliance
- Internal Audit
- Cybersecurity and Information Security
- Network Operations
- Data Protection and Privacy

Targeted Industries:

- Mobile Network Operators
- Fixed and Broadband Operators
- Internet Service Providers
- Satellite Communications Companies
- Mobile Virtual Network Operators
- Telecom Infrastructure Providers
- Data Centre and Cloud Providers
- Telecom Equipment Suppliers

Course Offerings:

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

- Interpret key Telecom Regulatory Framework requirements.
- Conduct a structured Telecom Risk Assessment.
- Build telecom risk and compliance registers.
- Identify regulatory, operational, cyber, privacy, and fraud risks.
- Define risk appetite, tolerance, ownership, and treatment actions.
- Strengthen Telecom Governance and Compliance controls.
- Improve Telecom Cybersecurity Compliance and Telecom Network Security.
- Evaluate Telecom Data Privacy Compliance requirements.
- Apply risk-based Telecom Audit and Compliance methods.
- Improve Telecom Fraud Risk Management.
- Support Telecom Business Continuity and incident reporting.
- Present risk and compliance information to management and regulators.

Training Methodology:

The course uses instructor-led discussions, telecom case studies, group exercises, risk scenarios, and compliance-mapping activities.

Participants examine real examples involving competition breaches, unfair pricing, privacy failures, network incidents, fraud, and operational disruption. They apply the ITU-T X.1055 risk cycle to assess risks, select controls, monitor effectiveness, and improve risk treatment.

NIST-based exercises help participants prioritize cybersecurity risks, assign risk owners, select responses, and complete risk registers.

Group activities include regulatory gap analysis, risk-register development, control evaluation, incident escalation, audit planning, and management reporting. Feedback sessions reinforce practical workplace application.

Course Toolbox:

- Telecom Risk Register Example
- Regulatory Compliance Checklist
- Telecom Risk Assessment Guide
- Compliance Gap-Analysis Template
- Risk Appetite and Tolerance Examples
- Telecom Control-Mapping Example
- Cybersecurity Risk Register Example

Course Agenda:

Day 1: Telecom Regulatory Framework and Compliance Governance

- **Topic 1:** Purpose and structure of the Telecom Regulatory Framework
- **Topic 2:** Roles of regulators, operators, competition authorities, and international bodies
- **Topic 3:** Licensing, spectrum, interconnection, and universal service obligations
- **Topic 4:** Telecommunications Regulatory Compliance across telecom services
- **Topic 5:** Telecom Governance and Compliance responsibilities
- **Topic 6:** Building an effective Telecom Compliance Management programme
- **Reflection & Review:** Map regulatory obligations and assign internal compliance ownership.

Day 2: Telecom Risk Management and Risk Assessment

- **Topic 1:** Principles of Telecommunications Risk Management
- **Topic 2:** Identifying telecom assets, systems, services, and third parties
- **Topic 3:** Telecom Risk Assessment using threats, vulnerabilities, likelihood, and impact
- **Topic 4:** Operational, network, information, physical, and compliance risks
- **Topic 5:** Risk appetite, tolerance, inherent risk, and residual risk
- **Topic 6:** Risk treatment, control selection, and continuous improvement
- **Reflection & Review:** Develop and prioritize telecom risk scenarios.

Day 3: Regulatory, Competition, Privacy, and Fraud Compliance

- **Topic 1:** Interaction between telecom regulation and competition law
- **Topic 2:** Price fixing, market sharing, information exchange, and restrictive agreements
- **Topic 3:** Dominant-position risks, unfair pricing, bundling, and infrastructure access
- **Topic 4:** Telecom Data Privacy Compliance for subscriber and traffic data
- **Topic 5:** Telecom Fraud Risk Management and revenue assurance
- **Topic 6:** Consumer protection, transparency, and service quality
- **Reflection & Review:** Assess a telecom conduct case and identify compliance risks.

Day 4: Cybersecurity Compliance and Operational Resilience

- **Topic 1:** Integrating Telecom Cybersecurity Compliance with enterprise risk
- **Topic 2:** Telecom Network Security and service-availability risks
- **Topic 3:** Cyber threats, unauthorized access, outages, and configuration failures
- **Topic 4:** Security controls, monitoring, access management, and incident response
- **Topic 5:** Telecom Business Continuity, redundancy, and disaster recovery
- **Topic 6:** Cyber incident escalation and regulatory notification
- **Reflection & Review:** Prioritize cyber risks and select suitable treatment actions.

Day 5: Telecom Audit, Monitoring, and Reporting

- **Topic 1:** Risk-based Telecom Audit and Compliance planning
- **Topic 2:** Compliance testing, evidence collection, and issue validation
- **Topic 3:** Key risk indicators, control metrics, and warning thresholds
- **Topic 4:** Third-party, supplier, outsourcing, and cloud risks
- **Topic 5:** Executive, board, and regulatory reporting
- **Topic 6:** Developing a Telecom Risk and Compliance improvement plan
- **Reflection & Review:** Present a consolidated risk profile and compliance action plan.

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

No formal qualifications are required. A basic understanding of telecom operations, regulation, risk, compliance, audit, cybersecurity, legal affairs, or network management is helpful.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans five days, approximately 20-25 hours of instruction.

What is the difference between telecom regulatory compliance and telecom risk management?

Telecom regulatory compliance focuses on meeting legal, licensing, competition, privacy, cybersecurity, and consumer obligations.

Telecom Risk Management has a broader scope and covers operational failures, network disruption, cyber incidents, fraud, supplier exposure, and reputational damage. The course integrates both disciplines so that compliance obligations are managed through structured risk assessment, controls, monitoring, and reporting.

How This Course is Different from Other Telecom Risk and Regulatory Compliance Courses:

This course combines regulatory compliance with practical risk management rather than treating them as separate subjects.

Participants examine licensing, competition, interconnection, cybersecurity, privacy, fraud, network resilience, audit, and business continuity within one integrated programme. The content uses telecom-specific ITU guidance for risk assessment, treatment, monitoring, and control improvement.

NIST guidance is also used to strengthen cybersecurity risk prioritization, ownership, response selection, and executive reporting.