Governance of Technology Risk Training Course

Professional Development Training Course Outline

Category	Corporate Governance	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Governance of Technology Risk Training Course is designed to equip professionals with advanced knowledge and practical strategies for managing technology-related risks in contemporary organizations. As digital transformation accelerates, the integration of emerging technologies introduces complex vulnerabilities that can affect operational resilience, regulatory compliance, and strategic decision-making. Participants will gain insights into risk assessment frameworks, cybersecurity governance, IT control mechanisms, and regulatory standards to strengthen organizational risk posture. The course emphasizes real-world applications, case studies, and industry best practices to prepare participants for proactive technology risk management.

In today's rapidly evolving digital landscape, technology risk governance has become a critical focus area for executives, IT managers, and compliance officers. This course explores the intersection of risk management, corporate governance, and technology innovation, highlighting trending risk areas such as cloud computing, AI adoption, data privacy, and cyber threats. Through interactive sessions, scenario-based learning, and actionable strategies, participants will be empowered to implement robust technology risk frameworks, ensure compliance with global standards, and align IT risk strategies with organizational objectives, fostering long-term resilience and value creation.

Programme Curriculum

Governance of Technology Risk Training Course

Introduction

Governance of Technology Risk Training Course is designed to equip professionals with advanced knowledge and practical strategies for managing technology-related risks in contemporary organizations. As digital transformation accelerates, the integration of emerging technologies introduces complex vulnerabilities that can affect operational resilience, regulatory compliance, and strategic decision-making. Participants will gain

insights into risk assessment frameworks, cybersecurity governance, IT control mechanisms, and regulatory standards to strengthen organizational risk posture. The course emphasizes real-world applications, case studies, and industry best practices to prepare participants for proactive technology risk management.

In today's rapidly evolving digital landscape, technology risk governance has become a critical focus area for executives, IT managers, and compliance officers. This course explores the intersection of risk management, corporate governance, and technology innovation, highlighting trending risk areas such as cloud computing, AI adoption, data privacy, and cyber threats. Through interactive sessions, scenario-based learning, and actionable strategies, participants will be empowered to implement robust technology risk frameworks, ensure compliance with global standards, and align IT risk strategies with organizational objectives, fostering long-term resilience and value creation.

Course Objectives

1. Develop a comprehensive understanding of technology risk governance frameworks and standards.
2. Identify emerging technology risks, including AI, cloud computing, and IoT vulnerabilities.
3. Implement effective IT risk assessment and mitigation strategies.
4. Enhance cybersecurity governance and control mechanisms across the organization.
5. Ensure regulatory compliance with global IT risk standards and data protection laws.
6. Integrate risk management strategies into business continuity and operational planning.
7. Utilize real-time risk monitoring tools and analytics for proactive decision-making.
8. Strengthen the board and executive reporting processes on technology risks.
9. Evaluate the effectiveness of existing IT policies, procedures, and controls.
10. Promote a risk-aware culture across IT and business functions.
11. Apply scenario-based testing and simulation exercises to anticipate potential threats.
12. Develop incident response and disaster recovery plans aligned with governance standards.
13. Benchmark organizational technology risk posture against industry best practices.

Organizational Benefits

- Improved alignment of IT risk strategy with business objectives.
- Reduced exposure to technology-related operational and regulatory risks.
- Enhanced decision-making through data-driven risk insights.
- Strengthened cybersecurity posture and IT control environment.
- Increased stakeholder confidence in IT governance and compliance.
- Improved regulatory compliance and audit readiness.
- Greater resilience against technology disruptions and cyber incidents.
- Enhanced organizational culture of risk awareness and accountability.
- Optimized IT resource allocation and investment in risk mitigation.
- Integration of emerging technologies with minimal operational risk.

Target Audiences

- Chief Information Officers (CIOs)
- IT Risk Managers
- Compliance and Governance Officers

- IT Auditors
- Cybersecurity Professionals
- Enterprise Risk Management Professionals
- Business Continuity and Disaster Recovery Managers
- Technology Consultants

Course Duration: 5 days

Course Modules

Module 1: Introduction to Technology Risk Governance

- Understanding technology risk and its organizational impact
- Key governance frameworks and standards
- Roles and responsibilities in IT risk governance
- Risk appetite and tolerance alignment with business objectives
- Case Study: Technology risk failures in multinational corporations
- Practical exercise: Mapping governance responsibilities

Module 2: IT Risk Assessment and Management

- Risk identification, analysis, and prioritization methods
- Emerging threats: AI, cloud, IoT, and data privacy risks
- Risk assessment tools and techniques
- Scenario-based risk evaluation
- Developing risk mitigation strategies
- Case Study: Risk assessment implementation in a banking environment

Module 3: Cybersecurity Governance

- Cybersecurity frameworks and control mechanisms
- Threat intelligence and vulnerability management
- Policy and compliance integration
- Incident management protocols
- Monitoring and reporting key risk indicators
- Case Study: Cyber breach response in a healthcare organization

Module 4: Regulatory Compliance and Data Protection

- Global IT compliance standards (ISO, NIST, GDPR, HIPAA)
- Legal and regulatory risk considerations
- Data privacy and protection strategies
- Compliance audits and reporting

- Continuous compliance monitoring
- Case Study: GDPR compliance implementation in a multinational firm

Module 5: Business Continuity and Disaster Recovery Planning

- Business continuity frameworks and planning principles
- Disaster recovery strategies and technology integration
- Risk-based prioritization of critical business functions
- Testing, simulations, and scenario planning
- Continuous improvement in continuity planning
- Case Study: Disaster recovery during a technology outage

Module 6: Technology Risk Monitoring and Reporting

- Key risk indicators and dashboards
- Risk reporting to executives and boards
- Real-time monitoring tools and analytics
- Integration of risk insights into strategic decisions
- Continuous improvement through feedback and audits
- Case Study: Monitoring risk in a financial services organization

Module 7: Risk Culture and Awareness

- Developing a risk-aware culture in IT and business teams
- Training and communication strategies
- Accountability and ownership of technology risks
- Measuring the effectiveness of awareness programs
- Continuous reinforcement through leadership and policies
- Case Study: Risk culture transformation in a tech startup

Module 8: Emerging Trends in Technology Risk

- AI, blockchain, cloud, and IoT risk management
- Predictive analytics for risk mitigation
- Future-proofing governance frameworks
- Integrating emerging tech with risk controls
- Strategic decision-making for technological innovation
- Case Study: Governance of AI adoption in global enterprises

Training Methodology

- Interactive lectures with real-world examples
- Case study analysis and group discussions
- Hands-on exercises and scenario simulations
- Risk assessment tools demonstration
- Role-playing exercises for governance responsibilities
- Q&A sessions for problem-solving and insights

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com