Compliance Management and Regulatory Risk in ERM Training Course

Professional Development Training Course Outline

Category	Risk Management	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern business landscape is characterized by unprecedented complexity and accelerated regulatory divergence, making robust Compliance Management and Regulatory Risk mitigation paramount to Enterprise Resilience. Organizations today operate under a constantly shifting matrix of global and local frameworks, from established regulations like GDPR and AML/KYC to emerging mandates around ESG (Environmental, Social, and Governance) and Trusted AI. A reactive approach to compliance is no longer tenable, as demonstrated by the potential for massive financial penalties and severe reputational damage from high-profile failures. Compliance Management and Regulatory Risk in ERM Training Course is designed to transition risk professionals from a siloed, check-the-box mentality to an integrated, proactive one, embedding compliance not as a cost center, but as a strategic enabler of long-term business value and a core pillar of Enterprise Risk Management (ERM)

This specialized program delivers a practical, hands-on framework for Risk-Based Compliance Management (RBCM), directly integrating regulatory requirements into the organization's overarching ERM architecture. Participants will master the use of modern risk tools, including GRC (Governance, Risk, and Compliance) platforms and AI-driven continuous monitoring, to establish a mature Risk Culture and ensure Operational Resilience. We will focus on tackling the most pressing challenges of the current era: managing Third-Party Risk (TPRM), governing the ethical and compliant deployment of Generative AI, and navigating the nuances of global sanctions and Financial Crime. By the end of this intensive training, attendees will possess the strategic acumen to proactively identify, assess, respond to, and report regulatory risks, thereby safeguarding the enterprise's mission and driving sustainable growth in an increasingly volatile world.

Programme Curriculum

Compliance Management and Regulatory Risk in ERM Training Course

Introduction

The modern business landscape is characterized by unprecedented complexity and accelerated regulatory divergence, making robust Compliance Management and Regulatory Risk mitigation paramount to Enterprise Resilience. Organizations today operate under a constantly shifting matrix of global and local frameworks, from established regulations like GDPR and AML/KYC to emerging mandates around ESG (Environmental, Social, and Governance) and Trusted AI. A reactive approach to compliance is no longer tenable, as demonstrated by the potential for massive financial penalties and severe reputational damage from high-profile failures. Compliance Management and Regulatory Risk in ERM Training Course is designed to transition risk professionals from a siloed, check-the-box mentality to an integrated, proactive one, embedding compliance not as a cost center, but as a strategic enabler of long-term business value and a core pillar of Enterprise Risk Management (ERM)

This specialized program delivers a practical, hands-on framework for Risk-Based Compliance Management (RBCM), directly integrating regulatory requirements into the organization's overarching ERM architecture. Participants will master the use of modern risk tools, including GRC (Governance, Risk, and Compliance) platforms and AI-driven continuous monitoring, to establish a mature Risk Culture and ensure Operational Resilience. We will focus on tackling the most pressing challenges of the current era: managing Third-Party Risk (TPRM), governing the ethical and compliant deployment of Generative AI, and navigating the nuances of global sanctions and Financial Crime. By the end of this intensive training, attendees will possess the strategic acumen to proactively identify, assess, respond to, and report regulatory risks, thereby safeguarding the enterprise's mission and driving sustainable growth in an increasingly volatile world.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Integrate Regulatory Compliance frameworks seamlessly into the existing Enterprise Risk Management (ERM) architecture.
2. Define and articulate the organization?ÇÖs Risk Appetite and Risk Tolerance specifically for regulatory and compliance risks.
3. Implement a Risk-Based Compliance Management (RBCM) methodology for efficient resource allocation and prioritization.
4. Apply a structured process for Regulatory Change Management (RCM) to proactively address new global and local legal obligations
5. Establish effective controls and Continuous Monitoring systems using RegTech and Compliance Automation tools.
6. Develop a robust program for Third-Party Risk Management (TPRM), mitigating supply chain and extended enterprise compliance vulnerabilities.
7. Analyze the ethical, legal, and operational risks associated with Trusted AI and implement an AI Governance framework to ensure algorithmic compliance and transparency.
8. Conduct comprehensive Compliance Risk Assessments focusing on high-impact areas like Financial Crime (AML/KYC) and anti-bribery (FCPA).
9. Measure and report on compliance effectiveness using objective metrics, including Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs).

10. Cultivate and promote a measurable, top-down Risk and Compliance Culture throughout the organization.
11. Design and test Operational Resilience and Business Continuity Plans (BCP) in response to regulatory mandates.
12. Manage and oversee Data Protection and Privacy compliance across multiple jurisdictions and mitigate breach-related regulatory penalties.
13. Lead internal investigations, manage regulatory inquiries, and implement corrective actions to prevent recurrence of Compliance Failures.

Target Audience

1. Chief Risk Officers (CROs) and ERM Leaders
2. Compliance Officers and Compliance Managers
3. Internal Auditors and External Auditors
4. Legal and Regulatory Affairs Professionals
5. Heads of Governance, Risk, and Compliance (GRC)
6. Information Security and Data Privacy Officers (CISO, DPO)
7. Senior Business Leaders accountable for operational units and controls
8. Third-Party Risk (TPRM) and Vendor Management Teams

Course Modules

Module 1: Foundations of ERM and Compliance Integration

- ERM Architecture and the Three Lines of Defense Model.
- Mapping Compliance Obligations to the Enterprise Risk Register.
- Defining and operationalizing the Risk Appetite Framework.
- Introduction to GRC Technology for unified risk oversight.
- Understanding the cost of non-compliance and strategic investment.
- Case Study: UBS (AML Failure) ?Çô Integrating financial crime compliance into global ERM structure.

Module 2: The Regulatory Change Management (RCM) Lifecycle

- Scanning and interpreting new global and local regulations
- Impact assessment and gap analysis of new rules.
- Prioritizing and resourcing implementation projects.
- Automating regulatory horizon scanning with RegTech tools.
- Tracking implementation and ensuring sign-off by accountable executives.
- Case Study: MiFID II/DORA Implementation ?Çô Proactive planning for large-scale financial services regulatory updates.

Module 3: Compliance Risk Assessment & Measurement

- Conducting a qualitative and quantitative Compliance Risk Assessment.
- Developing and monitoring Key Risk Indicators for early warning signals.
- Utilizing data analytics for identifying "near-misses" and control breakdowns.
- Designing and implementing effective Risk Control Self-Assessments.
- Aligning compliance metrics with corporate strategic objectives.
- Case Study: The Wells Fargo Scandal ?Çô Assessing and controlling sales-practices compliance risk.

Module 4: Anti-Money Laundering (AML) & Financial Crime Risk

- Deep dive into Know Your Customer and Customer Due Diligence protocols.
- Transaction monitoring and red-flag identification for suspicious activity reporting.
- Navigating global sanctions and export control compliance.
- Managing the risk of internal collusion and fraud.
- The role of AI/Machine Learning in detecting complex financial crime patterns.
- Case Study: HSBC/Deutsche Bank Failures ?Çô Inadequate controls and massive penalties for AML breaches.

Module 5: Data Protection and Privacy (DPP) Risk

- Core principles of GDPR, CCPA, and other global data privacy laws.
- The role and responsibilities of the Data Protection Officer (DPO).
- Implementing Privacy-by-Design and conducting Data Protection Impact Assessments (DPIA).
- Breach notification protocols and managing regulatory investigations.
- Governing data flows in a multi-jurisdictional cloud environment.
- Case Study: Meta/Facebook FTC Fine ?Çô Consequences of systemic failure in consumer data privacy controls.

Module 6: Third-Party Risk Management (TPRM)

- Establishing a risk-based framework for vendor and supplier due diligence.
- Continuous monitoring of fourth-party risk and supply chain compliance.
- Contractual protections, audit rights, and Service Level Agreements for compliance.
- Managing foreign corruption/bribery risk in the third-party ecosystem.
- Integration of TPRM data into the core ERM system.Case Study: Target Data Breach ?Çô Risk escalation via an HVAC vendor's weak security controls.

Module 7: AI Governance and Ethical Compliance

- Identifying the regulatory landscape for Trusted AI
- Addressing risks of algorithmic bias and discrimination.
- Ensuring data provenance and transparency in AI models.
- The human oversight and accountability model for AI-driven decisions.
- Developing an internal AI Governance Committee and charter.
- Case Study: Amazon's Hiring Tool Bias ?Çô Failure of an AI system due to inherent bias in the training data.

Module 8: Anti-Bribery and Corruption (ABC) Compliance

- Detailed review of the FCPA and the UK Bribery Act.
- Gift, hospitality, and expense policy controls and monitoring.
- Designing an effective ABC training and certification program.
- Conducting high-risk due diligence on agents and intermediaries.
- Managing whistleblower hotlines and internal investigations.
- Case Study: Siemens Bribery Scandal ?Çô Systemic corruption and the resulting global compliance overhaul.

Module 9: Compliance Culture and Training

- Defining and assessing the organization's Risk Culture Maturity.
- The role of senior leadership in setting the compliance mandate.

- Designing targeted, role-based compliance training and communication plans.
- Incentivizing ethical behavior and reporting.
- Integrating compliance ownership into performance reviews and compensation.
- Case Study: Enron's Ethical Failure ?Çô The consequence of a predatory culture on risk and compliance.

Module 10: Operational Resilience and Business Continuity

- Understanding new mandates for Operational Resilience
- Identifying and mapping critical business services and their Impact Tolerances.
- Scenario testing and stress testing for severe operational disruptions.
- Integrating IT Disaster Recovery and Business Continuity Planning with regulatory reporting.
- Maintaining service stability under extreme stress.
- Case Study: Cloud Outage Disruptions ?Çô Loss of critical services due to third-party or internal system failure and regulatory scrutiny.

Module 11: Compliance Reporting and Board Oversight

- Structuring impactful Compliance Dashboards for Executive Management.
- Developing a concise Board-Level Risk Report highlighting top regulatory exposures.
- The governance role and responsibilities of the Board's Audit/Risk Committee.
- Periodic review and assurance of the overall Compliance Management System.
- Effective communication of control failures and remediation progress.
- Case Study: Lehman Brothers/Global Financial Crisis ?Çô Board and executive failure to comprehend and manage aggregate risk.

Module 12: Internal Audit?ÇÖs Role in Compliance Assurance

- Aligning Internal Audit plans with the top-tier regulatory risks.
- Risk-Based Auditing methodology for control testing.
- Assessing the effectiveness and maturity of the CMS.
- The relationship between Internal Audit, Compliance, and the Chief Risk Officer.
- Reviewing remediation action plans and tracking closure of audit findings.
- Case Study: The Equifax Breach ?Çô Internal audit findings related to security patching and its failure to prevent the massive breach.

Module 13: Crisis Management and Regulatory Enforcement

- Developing a Crisis Response Playbook for regulatory events
- Managing communications with regulators, media, and the public.
- Conducting privilege-protected internal investigations.
- Negotiating settlements and implementing Corporate Monitorships.
- The process of self-reporting and demonstrating cooperation to mitigate penalties.
- Case Study: Uber Regulatory Concealment ?Çô The cost of hiding a data breach versus proactive disclosure.

Module 14: ESG and Sustainability Compliance

- Understanding emerging regulations around Environmental, Social, and Governance (ESG) reporting.
- Mitigating the risk of "Greenwashing" and misleading disclosures.
- Establishing controls for human rights and labor compliance in the supply chain.

- Integrating climate change and social risks into the ERM framework.
- Investor and stakeholder scrutiny on non-financial reporting.
- Case Study: Fashion Industry Supply Chain Violations ?Çô Social compliance failures leading to significant reputational and regulatory impact.

Module 15: Future of Compliance: RegTech and Automation

- Leveraging AI and Machine Learning for Continuous Control Monitoring.
- Utilizing Blockchain for immutable record-keeping and supply chain transparency.
- The shift from periodic auditing to Real-Time Compliance assurance.
- Evaluating and implementing Governance, Risk, and Compliance Platforms.
- The evolving skill set required for the Digital Compliance Officer.
- Case Study: Digital Transformation Failures ?Çô Regulatory fines resulting from poor migration of compliance processes to new systems

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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