RISK MANAGEMENT AND COMPLIANCE FOR CENTRAL BANKS COURSE

Introduction

Central banks operate at the heart of national and international financial systems, making effective risk management and regulatory compliance fundamental to monetary stability, financial-sector resilience, institutional credibility and public confidence. Their risk environment is increasingly complex, shaped by financial-market volatility, cyber threats, digital transformation, financial crime, geopolitical developments, operational disruptions and rapidly evolving regulatory expectations. The Risk Management and Compliance for Central Banks programme is a specialized 10-day professional programme designed to equip central banking and monetary authority professionals with the strategic knowledge and practical capabilities required to identify, assess, manage, monitor and mitigate risks across the institution. The programme takes an enterprise-wide and strategic approach, connecting risk management and compliance with central-bank mandates, governance, financial stability, banking supervision, reserves management, payment systems, operational resilience and institutional decision-making. Participants will explore how to establish robust risk governance structures, risk appetite frameworks, internal controls, compliance systems, financial crime controls and assurance mechanisms, while developing the ability to respond effectively to emerging and interconnected risks. Particular attention is given to the evolving risk landscape, including cybersecurity and technology risk, data governance, digital finance, sanctions risk, financial crime, business continuity, crisis management, climate-related financial risks and emerging systemic risks.The programme ultimately positions risk management and compliance not merely as control functions, but as strategic capabilities for safeguarding financial stability, protecting institutional integrity and strengthening confidence in the central bank and the wider financial system.

Course Objectives

- Understand the unique risk environment and compliance responsibilities of central banks.
- Develop and strengthen enterprise risk management frameworks.
- Establish effective risk governance, oversight and accountability structures.
- Develop risk appetite, tolerance and risk-limit frameworks.
- Identify, assess and priorities strategic, financial and operational risks.
- Strengthen financial, market, liquidity, credit and foreign-exchange risk management.
- Develop effective regulatory compliance and monitoring frameworks.
- Strengthen AML/CFT, sanctions and financial crime risk management.
- Enhance internal controls, assurance and risk-based audit processes.
- Manage cybersecurity, technology, data and digital-finance risks.
- Strengthen business continuity and operational resilience.
- Apply stress testing, scenario analysis and risk analytics.
- Strengthen crisis management and risk escalation mechanisms.
- Promote risk culture, ethics and institutional accountability.
- Integrate emerging risks into central-bank risk and compliance strategies.
- Develop practical strategies for strengthening institutional resilience and financial stability

Course Modules

> Module 1: The Central Bank Risk Environment
- Mandates and functions of modern central banks
- Strategic and institutional risk landscape
- Financial, operational and reputational risks
- Interconnectedness of central bank risks

> Module 2: Risk Governance and Institutional Accountability
- Risk governance structures and responsibilities
- Board, Governor and senior management oversight
- Risk committees and three-lines model
- Risk escalation and accountability mechanisms

> Module 3: Enterprise Risk Management Frameworks
- Principles of enterprise risk management
- Risk identification and classification
- Risk assessment and prioritization

- Risk treatment and monitoring

> Module 4: Risk Appetite, Tolerance and Risk Limits
- Developing a central bank risk appetite framework
- Risk capacity and risk tolerance
- Risk limits, thresholds and triggers
- Key Risk Indicators and risk reporting

> Module 5: Financial Risk Management
- Credit and counterparty risk
- Liquidity risk
- Interest-rate risk
- Central bank balance-sheet risks

> Module 6: Foreign Exchange and Reserves Risk Management
- Foreign-exchange risk
- Foreign reserves investment risks
- Sovereign and country risk
- Portfolio risk limits and stress testing

> Module 7: Operational Risk Management
- Operational risk identification and assessment
- People, process and systems risks
- Fraud and misconduct risks
- Third-party and outsourcing risks

> Module 8: Internal Controls and Assurance
- Internal control frameworks
- Control design and effectiveness
- Control self-assessment
- Assurance, remediation and follow-up

> Module 9: Central Bank Compliance Management
- Compliance governance frameworks
- Regulatory obligations and compliance risk
- Compliance monitoring and testing
- Compliance reporting and escalation

> Module 10: Legal and Regulatory Risk Management
- Legal and regulatory risk identification
- Regulatory change management
- Managing regulatory breaches
- Legal documentation and compliance assurance

> Module 11: AML/CFT Risk Management
- Money laundering and terrorist financing risks
- Risk-based AML/CFT frameworks
- AML/CFT controls and monitoring
- Reporting and regulatory coordination

> Module 12: Sanctions, Fraud and Financial Crime Compliance
- Sanctions risk assessment and controls
- Sanctions screening and escalation
- Fraud and corruption risk management
- Financial crime investigations and reporting

> Module 13: Risk-Based Banking Supervision
- Principles of risk-based supervision
- Institutional risk profiling
- On-site and off-site supervisory approaches
- Supervisory intervention and corrective measures

> Module 14: Systemic Risk and Financial Stability
- Systemic risk identification and measurement
- Financial-sector interconnectedness and contagion
- Macroprudential risk management
- Financial stability monitoring and stress testing

> Module 15: Cybersecurity and Technology Risk
- Cyber risk governance and assessment
- Critical infrastructure protection
- Cyber incident response and recovery
- Third-party technology and outsourcing risks

> Module 16: Data Governance and Digital Financial Risk
- Data governance and information integrity

- Data protection and privacy risks
- Digital finance and fintech risks
- Artificial intelligence and emerging technology risks

> Module 17: Business Continuity and Operational Resilience
- Business impact analysis
- Critical central bank functions
- Disaster recovery and continuity planning
- Operational resilience testing

> Module 18: Crisis Management and Risk Escalation
- Central bank crisis-management frameworks
- Crisis identification and escalation protocols
- Emergency decision-making and coordination
- Crisis communication and institutional recovery

> Module 19: Risk Analytics, Stress Testing and Emerging Risks
- Risk dashboards and Key Risk Indicators
- Scenario analysis and stress testing
- Early-warning systems and risk analytics
- Climate, geopolitical and emerging risks

> Module 20: Risk Culture, Ethics and Integrated Compliance Strategy
- Building a strong institutional risk culture
- Ethics, integrity and accountability
- Integrating risk management and compliance
- Developing a Central Bank Risk and Compliance Action Plan