

RISK MANAGEMENT FOR CREDIT INSTITUTIONS

Course Outline



18th November

RISK GOVERNANCE, CAPITAL ADEQUACY, ICAAP, RECOVERY PLANNING AND STRESS TESTING

- Understand a bank's risk management framework, including risk identification, assessment, monitoring and reporting.
- Understand how a Risk Appetite Framework operates through KRIs, limits and escalation processes.
- Assess a practical Risk Appetite Statement.
- Understand regulatory own funds, including CAR, Tier 1, CET1, AT1 and Tier 2 capital.
- Understand ICAAP methodology and SREP expectations.
- Assess capital management plans as a forward-looking tool for ensuring capital adequacy, strategic resilience and supervisory preparedness.
- Understand risk weight optimization strategies and how these may influence capital consumption, portfolio composition and strategic balance sheet decisions.
- Understand recovery plan requirements, stress testing frameworks, crisis governance and the use of a recovery simulation exercise

25th November

LIQUIDITY RISK, ILAAP, MARKET RISK, IRRBB AND BALANCE SHEET STRATEGY

- Assess liquidity adequacy using LCR, NSFR, intraday liquidity metrics, counterbalancing capacity and stress-testing results.
- Evaluate liquidity contingency and recovery readiness through triggers, escalation arrangements, funding options and operational testing.
- Apply ALM and IRRBB techniques to identify repricing, basis and behavioural risks across the balance sheet.
- Connect pricing decisions to balance-sheet risk by considering funding, liquidity, capital and return requirements.
- Develop and challenge NMD assumptions relating to behavioural maturity, repricing, runoff, segmentation and back-testing.
- Assess CSRBB and liquidity implications arising from spread, issuer, sector and liquidity shocks.
- Formulate business strategies by evaluating profitability, market opportunities, risk appetite, capital and liquidity constraints.
- Build and challenge three-year forecasts by incorporating business growth, strategic initiatives, financial constraints and stress scenarios.

1st December

OPERATIONAL RISK FRAMEWORK

- Apply operational risk management practices by maintaining risk frameworks, assessing exposures, analysing scenarios, tracking remediation actions and obtaining independent assurance.
- Strengthen operational resilience by identifying critical operations, assessing dependencies, setting recovery objectives, maintaining continuity arrangements and testing disruption scenarios.
- Implement DORA ICT risk management requirements through effective governance, risk identification, security controls, incident response, recovery planning and continuous improvement.
- Establish a risk-based digital operational resilience testing programme covering vulnerability assessments, penetration testing, scenario testing and critical ICT systems.
- Manage operational and ICT incidents through effective detection, classification, investigation, remediation and regulatory reporting processes.
- Manage outsourcing and ICT third-party risk through due diligence, contractual oversight, ongoing monitoring, regulatory compliance and exit planning.
- Develop integrated policy governance arrangements that ensure clear ownership, control requirements, regulatory alignment, review processes and assurance activities.