



Operational Risk Management and Operational Resilience Training Course



Operational Risk Management and Operational Resilience Training Course

Introduction:

Operational risk management and operational resilience is a 10-day course for operational risk, internal control, compliance and business line risk functions in banks, insurers and corporates that ends with an operational risk framework and resilience self-assessment for a case institution. Many institutions run RCSA workshops, loss logs and continuity plans as separate exercises, so control gaps, recurring losses and fragile business services reach the board too late. Nominees already record risks or test controls in their units, and the course is taught through case studies on bank, insurer and corporate material. CoreConcept Training Center delivers this operational risk management course.

Course Objectives:

- Classify operational risk events using the Basel definition and the seven event types, and assign governance roles across the three lines of defence
- Facilitate RCSA workshops and build risk and control matrices from mapped processes
- Collect and analyse internal and external loss event data to locate root causes and control weaknesses
- Design operational risk scenarios and explain how loss history feeds operational risk capital under the standardised approach
- Assess third-party, technology, cyber and conduct risk exposures and track the resulting issues to closure
- Identify important business services, set impact tolerances and report operational risk and resilience to management and the board

Target Audience:

- Operational risk functions responsible for the framework, the RCSA cycle and loss event data
 - Enterprise risk functions that consolidate operational risk into the wider risk profile
 - Compliance and internal control functions that test controls and follow remediation
 - Business line risk champions who run self-assessments and record loss events in their units
 - Technology, outsourcing and resilience coordinators who map dependencies behind important business services
-

Course Outline:

Day 1: Operational Risk Foundations and Event-Type Taxonomy

- Basel Operational Risk Definition and Its Boundaries
- Seven Basel Event Types as a Loss Taxonomy
- Cause, Event and Impact Classification Using Bow-Tie Logic
- Operational Risk Versus Credit, Market and Strategic Risk
- Operational Risk Maturity Baseline Checklist for an Institution

Day 2: Governance, Basel Principles and the Three Lines of Defence

- Basel Principles for Sound Operational Risk Management Overview
- ISO 31000 Process Applied to Operational Risk Cycles
- Three Lines of Defence Roles for Operational Risk
- Operational Risk Committee Charter and Escalation Routes
- Business Line Risk Champion Network and RACI Matrix

Day 3: Risk and Control Self-Assessment and Process Mapping

- RCSA Workshop Planning, Facilitation and Scoring Scales
- Process Mapping With SIPOC and Swimlane Diagrams
- Risk and Control Matrix Construction for Key Processes
- Control Design and Operating Effectiveness Testing Criteria
- Inherent and Residual Rating Calibration Across Business Lines

Day 4: Internal Loss Data, External Loss Data and Indicators

- Internal Loss Event Data Collection Thresholds and Fields
- Near Misses, Boundary Events and Recovery Recording Rules
- External Loss Data Consortia and Public Loss Databases
- Root Cause Analysis of Loss Events With Five Whys
- Key Risk Indicator Linkage to RCSA and Loss Findings

Day 5: Guided Case Study on Week-One Operational Risk Tools

- Retail Bank Payments Process RCSA Case Exercise
 - Insurance Claims Loss Event Classification Case Exercise
 - Corporate Procurement Control Gap Case Analysis
 - Risk and Control Matrix Review Against Loss History
 - Week-One Findings Consolidation Into an Operational Risk Profile
-

Day 6: Scenario Analysis and Operational Risk Capital Concepts

- Scenario Analysis Workshop Design and Expert Elicitation
- Severity and Frequency Estimation for Tail Loss Scenarios
- Scenario Bias Challenge Using Loss Data Benchmarks
- Standardised Approach Business Indicator Component at Overview Level
- Internal Loss Multiplier and Ten-Year Loss History Concepts

Day 7: Third-Party, Technology, Cyber and Conduct Risk Interfaces

- Third-Party and Outsourcing Risk Inventory and Tiering
- ICT and Cyber Risk Interface With Operational Risk
- Change Management Risk Assessment for New Products and Systems
- Conduct Risk Indicators and Customer Outcome Reviews
- Issues and Action Management Log With Validation Steps

Day 8: Operational Resilience of Important Business Services

- Important Business Service Identification and Prioritisation Criteria
- Impact Tolerance Setting for Severe but Plausible Disruption
- Mapping People, Processes, Technology, Facilities and Third Parties
- Resilience Scenario Testing Against Impact Tolerances
- Resilience Communication Plan for Customers and Counterparties

Day 9: Reporting, Benchmarking and Continuous Improvement

- Operational Risk Dashboard Design for Management Committees
- Board Operational Risk and Resilience Report Structure
- Resilience Vulnerability Remediation Plan and Investment Prioritisation
- Operational Risk Framework Maturity Benchmarking Scorecard
- Lessons Learned Review After Incidents and Test Exercises

Day 10: Capstone Case Study on an Operational Risk Framework and Resilience Self-Assessment

- Case Institution Data Pack and Team Role Allocation
 - RCSA, Loss Data and Scenario Results Applied to the Case
 - Important Business Service Mapping Applied to the Case Institution
 - Board Report Drafting From the Case Findings
 - Operational Risk Framework and Resilience Self-Assessment Completion
-

Skills You Will Gain:

- Operational Risk Taxonomy Design
- Self-Assessment Moderation
- Control Effectiveness Testing
- Loss Event Root Cause Analysis
- Tail Scenario Estimation
- Outsourcing Risk Tiering
- Disruption Tolerance Calibration
- Board Risk Narrative Writing

Why Attend This Course:

- Deliver an operational risk framework and resilience self-assessment for a case institution to the head of operational risk and the risk committee
- Decide which control gaps, loss trends and scenario results warrant escalation and which actions close them
- Avoid repeat losses and breaches of impact tolerance caused by untested controls and unmapped third-party dependencies
- Share RCSA templates, loss data fields and service mapping methods with risk champions in other units

Conclusion:

Back at work, the participant hands the operational risk framework and resilience self-assessment to the head of operational risk, the risk committee and business line owners, who use it to agree priority control fixes, approve impact tolerances for important business services and set the next RCSA cycle. Risk champions apply the same loss data fields, scenario templates and issues log across their units. After the first quarterly report, the institution should review whether loss records, indicators and test results matched the self-assessment and adjust ratings and tolerances accordingly.

Frequently Asked Questions FAQ:

What should participants know before the operational risk management and operational resilience course?

Participants should already record risks, test controls or support risk reporting in a bank, insurer or corporate. Basic familiarity with risk registers helps. Bringing an anonymised process map, loss log or RCSA template lets them apply the methods to their own unit.

How does operational risk management and operational resilience differ from an enterprise risk management or business continuity course?

It concentrates on the tools of the operational risk function, namely RCSA, loss data, scenarios and issue tracking, and on the resilience of important business services. Enterprise-wide frameworks, risk appetite calibration and continuity management systems appear only at overview level.

Why does operational risk management and operational resilience rely on loss event data?

Loss event data shows where controls actually failed, how often and at what cost. It tests RCSA ratings, informs scenario severity estimates and, for banks, feeds the internal loss component of operational risk capital under the standardised approach.

What does a participant take back from the operational risk management and operational resilience course?

Participants take back an operational risk framework and resilience self-assessment, with RCSA and loss data templates, a scenario worksheet, an issues log and a board report structure that can be adapted to their own institution.
