JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Operational Risk and Resilience in Finance Training Course

2 – 13 May 2027
Kuala Lumpur

jupiterprime.uk
info@jupiterprime.uk
Registered in the United Kingdom and Saudi Arabia

Operational Risk and Resilience in Finance Training Course

Ref: 264_8468 **Date:** 2 – 13 May 2027 **Location:** Kuala Lumpur **Fees:** 8000 GBP

Operational Risk and Resilience in Finance is a 2-week training course for operational risk officers in banks, insurers and asset managers who collect loss events, run control assessments and test how critical services withstand disruption, and it ends with a Loss Scenario and Resilience Pack. Payment outages, outsourcing failures and fraud events now reach customers within minutes, and supervisors expect firms to prove they can stay within tolerance. Jupiter Prime Training runs this course on operational risk and resilience in finance.

Why Operational Risk and Resilience in Finance Matters Now

Three groups are reshaping this discipline. Supervisors increasingly judge financial firms on whether important services survive severe but plausible disruption, not only on capital held. Cloud providers, fintech partners and outsourced processors now carry a large share of critical activity, so a vendor failure becomes the firm's incident. Customers switch quickly after an outage or a mis-sold product. Firms that capture losses honestly and map their service dependencies recover faster and allocate capital more accurately; those that do not repeat the same failures. The course draws on Basel Committee on Banking Supervision BCBS guidance on operational risk and the ISO 31000 risk management guidelines.

Who Gains Most from Operational Risk and Resilience in Finance

- Operational risk leads who own the loss event database and its taxonomy across business lines
- Second-line specialists who facilitate risk and control self-assessments in retail, corporate and markets units
- Resilience and continuity heads who set impact tolerances for critical customer services
- Vendor and outsourcing risk owners who assess material third parties and concentration exposure
- Capital and model analysts who turn loss and scenario data into capital estimates

A cross-functional group from one institution, combining operational risk, resilience and vendor oversight, gains most because it can join loss data, scenarios and service maps into one view.

Operational Risk and Resilience in Finance Capabilities

Participants learn to treat failed processes, people, systems and suppliers as measurable exposures that can be captured, rated, stressed and connected to capital and service continuity.

- Design a loss event taxonomy and capture standard that ensures complete, consistent records — operational risk committee
- Facilitate a risk and control self-assessment that produces challengeable ratings — business line heads
- Calibrate key risk indicators with thresholds linked to the firm's tolerance — chief risk officer
- Build severe but plausible scenarios and estimate their frequency and severity — capital planning and ICAAP owners
- Assess material third parties for concentration, exit and substitution risk — procurement and board risk committee
- Test important business services against impact tolerances — executive owners and supervisors

Key Operational Risk and Resilience in Finance Terms

- Operational risk — the risk of loss from inadequate or failed internal processes, people and systems, or from external events.
- Loss event data — a structured record of operational failures with dates, amounts, causes and recoveries used for analysis and capital.
- RCSA — risk and control self-assessment, a facilitated exercise in which business units rate their exposures and control effectiveness.
- Important business service — a service whose disruption would cause intolerable harm to customers or market integrity.
- Impact tolerance — the maximum disruption, often in time, an important business service can sustain before harm becomes intolerable.
- Concentration risk — exposure arising when many critical activities depend on a single supplier, platform or location.

Operational Risk and Resilience in Finance Day by Day

Day 1: The Operational Risk Landscape in Financial Firms

- BCBS Operational Risk Principles — Setting Expectations For Banks And Insurers
- Basel Event-Type Categories — Classifying Fraud, Process And System Failures
- Lessons From Rogue Trading And Payment Outages — Root Patterns
- Operational Risk Framework Components — Policy, Tools And Committees
- Retail Banking Versus Asset Management Profiles — Contrasting Exposures

Day 2: Loss Event Data Collection

- Loss Capture Thresholds — Deciding What Must Be Recorded
- Gross, Net And Recovery Fields — Ensuring Comparable Loss Values
- Boundary Events With Credit And Market Risk — Avoiding Double Counting
- Near-Miss And Rapid Recovery Logging — Widening The Evidence Base
- Data Quality Reconciliation To The General Ledger — Proving Completeness

Day 3: Risk and Control Self-Assessment

- RCSA Workshop Facilitation — Structuring Challenge Across Business Lines
- Process Taxonomy Alignment — Linking Exposures To Products And Channels
- Inherent And Residual Rating Scales — Rating Exposures Consistently
- Control Testing Evidence — Separating Asserted From Demonstrated Effectiveness
- Second-Line Challenge Log — Recording Disagreements And Resolutions

Day 4: Key Risk Indicators

- KRI Selection Criteria — Choosing Predictive Over Descriptive Metrics
- Threshold Setting Methods — Statistical, Expert And Tolerance-Based Limits
- KRI Dashboards For Insurers — Claims Backlogs And Underwriting Errors
- KRI Dashboards For Banks — Failed Trades, Reconciliation Breaks And Fraud
- Escalation Rules — Triggering Action When Indicators Breach

Day 5: Scenario Analysis

- Scenario Workshop Design — Selecting Severe But Plausible Events
- Frequency And Severity Elicitation — Structuring Expert Estimates
- Bias Controls In Scenario Panels — Avoiding Anchoring On Recent Losses
- Combining Internal, External And Scenario Data — Building A Fuller Picture
- Scenario Documentation Standards — Supporting Validation And Audit

Day 6: Operational Risk Capital Concepts

- Standardised Approach Concepts — Business Indicator And Loss Component Logic
- Loss Distribution Approach — Modelling Frequency And Severity For Capital
- ICAAP And ORSA Integration — Placing Operational Risk In Capital Plans
- Insurance Offsets And Mitigation Recognition — Judging Credit For Cover
- Capital Allocation To Business Lines — Influencing Pricing And Behaviour

Day 7: Outsourcing and Third-Party Risk

- Third-Party Inventory And Criticality Tiering — Focusing Oversight Effort
- Due Diligence And Contract Clauses — Audit Rights, Exit And Data Return
- Cloud And Fintech Dependency Mapping — Seeing Fourth-Party Chains
- Concentration And Substitutability Analysis — Planning For Provider Failure
- Ongoing Vendor Performance Monitoring — Detecting Deterioration Early

Day 8: Operational Resilience

- Important Business Service Identification — Prioritising What Customers Need Most
- Impact Tolerance Setting — Defining Maximum Tolerable Disruption
- Service Mapping — People, Processes, Technology, Facilities And Suppliers
- Resilience Scenario Testing — Cyber, Data Centre And Supplier Outages
- Self-Assessment Documentation — Evidencing Resilience To The Board

Day 9: Incidents, Conduct and Reporting

- Incident Classification And Root Cause — Learning From Each Failure
- Conduct And Mis-Selling Events — Linking Operational Failures To Customer Harm
- Operational Risk Committee Reporting — Profile, Trends And Actions
- Board Risk Committee Packs — Presenting Tolerance Breaches And Remediation
- Remediation Tracking — Closing Findings With Verified Evidence

Day 10: Practising the Loss Scenario and Resilience Pack

- Applying Loss Data Analysis — Profiling A Case Bank's Event History
- Applying RCSA And KRIs — Rating And Monitoring A Payments Process
- Applying Impact Tolerances — Testing A Disrupted Claims Service
- Peer Challenge Panel — Defending Scenario Estimates And Assumptions
- Loss Scenario And Resilience Pack — Assembling Scenarios, Tolerances And Actions

Applying Operational Risk and Resilience in Finance After the Course

- Reconcile the last quarter's loss events against the general ledger and present the gaps and corrected taxonomy to the operational risk committee.
- Run a mapping session for one important business service, identify its critical suppliers and propose an impact tolerance for executive approval.

Operational Risk and Resilience in Finance Questions FAQ

What is operational risk and resilience in finance and why does it matter now?

Operational risk and resilience in finance covers losses from failed processes, people, systems and suppliers, and the ability to keep critical services running. It matters now because outages and vendor failures hit customers instantly and supervisors expect proof of resilience.

Which roles gain most from operational risk and resilience in finance training?

Operational risk officers in banks, insurers and asset managers gain most, along with resilience leads, vendor risk owners and capital analysts who depend on reliable loss and scenario data for their decisions.

How does operational risk and resilience in finance differ from an enterprise risk quantification course?

Operational risk and resilience in finance focuses on the tools financial firms use for non-financial losses, such as loss databases, RCSA, capital concepts and service tolerances. An enterprise risk quantification course covers modelling methods across all exposure types and sectors.

What do you bring back from operational risk and resilience in finance training?

You bring back a pack of severe but plausible scenarios with estimates, impact tolerances for a critical service and an action list. You also return with templates for loss capture, RCSA and indicator thresholds.

Operational Risk and Resilience in Finance: The Way Forward

The Loss Scenario and Resilience Pack first informs whether current capital and continuity investment match the firm's most severe plausible failures. Operational risk and resilience leads use it with business owners and the board risk committee. After its first use, revisit third-party dependencies, as service maps often reveal suppliers that scenarios had not yet considered.