Operational Risk Management in Banking & Financial Institutions

11 - 15 Oct 2026
Kuala Lumpur (Malaysia)

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Operational Risk Management in Banking & Financial Institutions

Ref.: 16174_1009412 **Date:** 11 - 15 Oct 2026 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4600 **Euro**

Introduction:

Operational risk is one of the most significant challenges facing today’s banking and financial sectors, impacting everything from compliance to customer confidence. This Operational Risk Management in Banking and Financial Institutions training course provides a deep understanding of how to identify, assess, mitigate, and monitor operational risks in complex financial environments. Participants will explore core frameworks, international standards, and regulatory expectations that shape modern operational risk governance.

Real-world case studies and industry-specific examples will be used to ensure the application of theory into practice. The Operational Risk Management in Banking and Financial Institutions course focuses on emerging risks, including cyber threats, third-party risk, and challenges associated with digital transformation. Participants will use proactive risk management strategies that align with institutional resilience and business continuity. They will possess the tools to support sustainable operations and regulatory compliance in an evolving financial ecosystem.

Targeted Groups:

This Operational Risk Management in Banking and Financial Institutions training targets professionals seeking specialized knowledge and skills:

- Risk management professionals in banks.
- Compliance officers and audit staff.
- Heads of operational departments in financial institutions.
- Professionals from central banks and regulatory authorities.
- Risk analysts and internal control teams.
- Banking professionals transitioning into risk functions.
- Consultants and advisors in the banking sector.
- Staff responsible for business continuity and disaster recovery.
- Professionals involved in digital banking and fintech risk.
- Senior executives aim to strengthen governance frameworks.

Targeted Competencies:

Participants will gain the following competencies during the Operational Risk Management in Banking and Financial Institutions program:

- Strong ability to identify and categorize operational risks.
- Competence in developing risk assessment tools.
- Understanding of Basel compliance and risk regulation.
- Capability to create mitigation and control frameworks.
- Skill in monitoring key risk indicators KRIs.
- Ability to conduct root cause analysis for incidents.
- Proficiency in integrating operational risk with governance.
- Clear communication of risk strategies and findings.
- Leadership in building a risk-aware organizational culture.

Course Objectives:

Participants will achieve the following objectives by completing the Operational Risk Management in Banking and Financial Institutions course:

- Define operational risk and its components within the banking context.
- Identify major categories and sources of operational risk.
- Analyze risk events and effectively evaluate their root causes.
- Develop risk assessment frameworks tailored to the financial services industry.
- Measure operational risk using qualitative and quantitative approaches.
- Design effective mitigation plans to reduce institutional exposure.
- Apply global regulatory requirements, including Basel III/IV guidelines.
- Monitor operational risk indicators to support strategic decision-making.
- Evaluate the effectiveness of internal controls and risk culture.
- Integrate risk management into business planning and governance.
- Recommend risk reporting structures aligned with stakeholder needs.
- Assess emerging threats such as cyberattacks and third-party failures.
- Construct incident reporting mechanisms and loss data collection systems.
- Communicate risk strategies clearly across organizational levels.
- Promote a proactive culture of risk awareness and accountability.

Course Content:

Unit 1: Foundations of Operational Risk in Banking:

- Definition, scope, and importance of operational risk.
- Evolution of operational risk management in finance.
- Comparison between operational, credit, and market risk.
- Regulatory background: Basel II, III, and IV perspectives.
- Operational risk events: real-world cases and lessons learned.
- Types of operational risk: process, people, systems, and external events.
- Role of senior management and board oversight.
- Risk appetite and risk tolerance statements.
- Operational risk in the age of digital banking and fintech.

Unit 2: Risk Identification and Assessment Techniques:

- Tools for identifying operational risk events and scenarios.
- Risk self-assessments and workshops: methodology and execution.
- Process mapping and identifying control gaps.
- Root cause analysis for incident investigation.
- Scenario analysis and stress testing.
- Developing and using Risk Control Self-Assessments RCSAs.
- External Loss Data: Sources, Benchmarking, and Adaptation.
- Using internal audit reports to enhance risk identification.
- Risk prioritization based on likelihood and impact.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 3: Risk Measurement, Mitigation, and Monitoring:

- Qualitative vs. Quantitative Measurement of Operational Risk.
- Key Risk Indicators KRIs: development and use.
- Loss event data collection and classification.
- Building operational risk models and metrics.
- Control design and assessment of effectiveness.
- Mitigation strategies: preventive, detective, and corrective controls.
- Action plans and control testing procedures.
- Using technology for real-time risk monitoring.
- Early Warning Systems and Dashboards for Executives.

Unit 4: Regulatory Compliance and Governance Integration:

- Regulatory Expectations for Operational Risk in Banking
- Basel III and IV operational risk capital requirements.
- Enterprise Risk Management ERM and its connection to operational risk.
- Role of compliance and internal audit functions.
- Reporting Lines and Governance Structure Best Practices.
- Integration of operational risk in strategy and planning.
- Managing third-party and outsourcing risks.
- Role of Chief Risk Officer CRO and risk committees.
- Internal reporting and regulatory disclosures.

Unit 5: Emerging Operational Risks and Business Resilience:

- Cybersecurity threats and data breach management.
- Operational resilience and crisis response frameworks.
- Business continuity planning and disaster recovery.
- Risk associated with remote work and cloud banking.
- ESG-related operational risks and reputational impact.
- Fraud risk management and anti-money laundering.
- Managing technological disruptions and legacy systems.
- Digital transformation and its operational risks.
- Creating a culture of risk transparency and learning.

Final Insights & Key Takeaways:

This Operational Risk Management in Banking and Financial Institutions course offers an examination of managing operational risk within the dynamic banking and financial services landscape. Participants leave with the practical tools and strategic vision to drive operational risk governance and compliance. A proactive, structured approach to risk mitigation helps build organizational resilience and regulatory alignment. The knowledge gained positions professionals to navigate traditional and emerging risk challenges with confidence.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Registration form on the :
Operational Risk Management in Banking & Financial Institutions

code: 16174 **From:** 11 - 15 Oct 2026 **Venue:** Kuala Lumpur (Malaysia) **Fees:** 4600 **Euro**

Complete & Mail or fax to Mercury Training Center at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng):
....
Position:
....
Telephone / Mobile:
....
Personal E-Mail:
....
Official E-Mail:
....

Company Information

Company Name:
....
Address:
....
City / Country:
....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng):
....
Position:
....
Telephone / Mobile:
....
Personal E-Mail:
....
Official E-Mail:
....

Payment Method

☐ Please invoice me

☐ Please invoice my company