Operational Risk Management & Resilience Mastery Program

2027 □□□□□□ 5 – 1
Munich (Germany)



Operational Risk Management & Resilience Mastery Program

Ref: 20220627_205808 Location: Munich (Germany) Fees: 5200 GBP

Why This Course

Finance organizations operate in an environment where uncertainty, disruption, regulatory pressure, cyber threats, market volatility, and reputational risks can quickly affect performance and stability. Operational risk is no longer limited to internal process failures. It now includes technology disruption, third-party dependencies, cybersecurity exposure, crisis response capability, data protection, and the organization's ability to remain resilient under pressure.

For finance professionals, managing risk effectively requires a structured approach to identifying vulnerabilities, assessing exposure, implementing controls, and preparing for situations where preventive measures may not be enough. Strong operational risk management must also be supported by resilience planning, crisis readiness, governance, communication, and a culture where risk awareness is part of everyday decision-making.

This intensive 1-week program equips finance professionals with the knowledge, tools, and practical techniques needed to manage operational risk and strengthen organizational resilience. Through frameworks, case studies, assessment tools, simulations, and action planning, participants will learn how to identify and mitigate risks, respond to crises, improve cybersecurity awareness, and embed risk management into organizational processes.

What You'll Learn and Practice

By joining this program, you will:

- Understand operational risk concepts, terminology, and frameworks.
- Identify strategic, financial, operational, reputational, cyber, and information-related risks.
- Apply practical risk identification and assessment techniques.
- Develop effective mitigation strategies and control measures.
- Understand resilience and its importance in the financial sector.
- Use risk and resilience assessment tools to evaluate organizational readiness.
- Develop proactive measures to strengthen business continuity and resilience.
- Apply crisis management principles when risk controls are insufficient.
- Build and use a crisis management playbook.
- Understand common IT and cybersecurity threats in finance.
- Improve cyber risk posture and protect sensitive data.
- Support intellectual property and information asset protection.
- Build a risk-aware culture, governance structure, and communication approach.
- Develop a comprehensive operational risk and resilience strategy.



The Program Flow

Day 1: Foundations of Operational Risk Management

- Introduction to operational risk concepts and terminology.
- Understanding operational risk in the financial sector.
- Sources of risk: people, processes, systems, external events, technology, and third parties.
- Risk identification and assessment techniques.
- Operational risk frameworks and best practices.
- Controls, mitigation strategies, and risk ownership.
- Case study: Applying a systematic operational risk management process.

Day 2: Building Organizational Resilience

- Defining resilience in financial organizations.
- Understanding the connection between operational risk, continuity, and resilience.
- Strategies for enhancing organizational resilience.
- Using the SPECTRA risk and resilience assessment tool.
- Identifying vulnerabilities, dependencies, and critical functions.
- Developing proactive resilience measures.
- Workshop: Building a resilience improvement plan for a selected business area.

Day 3: Crisis Management and Response

- Crisis management principles, stages, and success factors.
- Understanding how crises develop and escalate.
- Analyzing financial crises and their operational, reputational, and regulatory impacts.
- Roles, responsibilities, escalation, and decision-making during crises.
- Developing an effective crisis management playbook.
- Communication strategies during crisis situations.
- Simulation: Crisis response, decision-making, and lessons learned.

Day 4: Cybersecurity and Information Risk Management

- Common IT and cybersecurity threats in finance.
- Cyber risk, data breaches, fraud, ransomware, insider threats, and third-party exposure.
- Evaluating and improving cyber risk posture.
- Implementing cybersecurity best practices and control measures.
- Protecting intellectual property and sensitive information.
- Data classification, access control, awareness, and incident response.
- Practical exercise: Developing a cyber and information risk action checklist.



Day 5: Embedding Risk Management and Resilience

- Creating a risk-aware culture and governance structure.
- Defining accountability, ownership, oversight, and reporting lines.
- Integrating risk management into organizational processes and decision-making.
- Effective risk communication strategies for executives, teams, and stakeholders.
- Monitoring, reporting, and improving risk and resilience performance.
- Developing a comprehensive risk management and resilience strategy.
- Final activity: Presenting an operational risk and resilience implementation roadmap.

Individual Impact

- Strengthen your understanding of operational risk and resilience in finance.
- Improve your ability to conduct structured risk assessments.
- Build confidence in developing mitigation strategies and control actions.
- Gain practical crisis management and decision-making skills.
- Improve awareness of cybersecurity, information risk, and data protection.
- Develop tools to communicate risk clearly and support better decisions.

Work Impact

- Improve the organization's ability to identify, assess, and mitigate operational risks.
- Strengthen resilience against disruption, crisis, and uncertainty.
- Improve crisis readiness through structured playbooks and response planning.
- Reduce exposure to cyber threats and sensitive data risks.
- Support stronger governance, accountability, and risk ownership.
- Build a more proactive risk-aware culture across teams and functions.

Training Methodology

This program uses a practical and finance-focused approach to help participants apply risk and resilience tools in real organizational contexts. Learning methods include:

- Interactive discussions and guided facilitation.
- Financial sector risk and crisis case studies.
- Operational risk identification and assessment exercises.
- Risk mitigation and control planning workshops.
- SPECTRA-style resilience assessment activities.
- Crisis response simulations and decision-making exercises.
- Cybersecurity and information risk scenarios.
- Group work, peer feedback, and practical action planning tools.



Beyond the Course

Upon completion, participants will be prepared to manage operational risk and strengthen resilience with greater structure, confidence, and strategic awareness. They will return ready to:

- Conduct thorough operational risk assessments.
- Develop practical mitigation strategies and control measures.
- Create and implement a crisis management playbook.
- Strengthen cybersecurity awareness and information protection.
- Foster a risk-aware culture within their organization.
- Build a comprehensive risk management and resilience strategy that supports long-term stability and performance.

