Crisis Response for Operational Risk Managers Training Course

Professional Development Training Course Outline

Category	Risk Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Crisis Response for Operational Risk Managers Training Course is specifically engineered for a new era of complex, interconnected risk. Traditional risk models are insufficient against today's threats, from sophisticated cyberattacks to geopolitical instability and climate-driven disruptions. Operational Risk Managers must transition from reactive damage control to proactive, holistic crisis leadership to ensure organizational resilience and business continuity. This course provides the strategic frameworks, real-time decision-making tools, and advanced scenario planning techniques necessary to protect critical operations, safeguard stakeholder trust, and maintain a decisive advantage in the face of sudden, severe disruption.

Participants will gain mastery over the entire crisis lifecycle from anticipating emerging risks and establishing robust operational resilience to executing a high-stakes response and driving post-crisis organizational learning. We emphasize practical application through immersive simulations and deep-dive case studies focusing on modern threats like supply chain shocks, data breaches, and conduct risk. By integrating a forward-looking risk culture with a structured crisis management playbook, this program empowers Operational Risk Managers to become the essential architects of their organization’s long-term stability and sustained performance.

Programme Curriculum

Crisis Response for Operational Risk Managers Training Course

Introduction

Crisis Response for Operational Risk Managers Training Course is specifically engineered for a new era of complex, interconnected risk. Traditional risk models are insufficient against today's threats, from sophisticated cyberattacks to geopolitical instability and climate-driven disruptions. Operational Risk Managers must transition from reactive damage control to proactive, holistic crisis leadership to ensure organizational resilience and

business continuity. This course provides the strategic frameworks, real-time decision-making tools, and advanced scenario planning techniques necessary to protect critical operations, safeguard stakeholder trust, and maintain a decisive advantage in the face of sudden, severe disruption.

Participants will gain mastery over the entire crisis lifecycle from anticipating emerging risks and establishing robust operational resilience to executing a high-stakes response and driving post-crisis organizational learning. We emphasize practical application through immersive simulations and deep-dive case studies focusing on modern threats like supply chain shocks, data breaches, and conduct risk. By integrating a forward-looking risk culture with a structured crisis management playbook, this program empowers Operational Risk Managers to become the essential architects of their organization’s long-term stability and sustained performance.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Define and embed an Operational Resilience framework aligned with regulatory expectations
2. Conduct advanced scenario analysis and stress testing for severe but plausible operational disruptions.
3. Establish tolerances for disruption for critical business services and map end-to-end dependencies.
4. Implement a rapid Crisis Activation Protocol (CAP) for immediate, effective response to high-impact events.
5. Master real-time decision-making under pressure using structured leadership and command-and-control models.
6. Develop an effective crisis communication strategy to manage internal and external stakeholder trust and reputation.
7. Mitigate Third-Party Risk (TPR) and ensure the continuity of services from critical vendors and supply chains.
8. Conduct comprehensive Root Cause Analysis (RCA) for operational failures to drive continuous improvement.
9. Identify and track Key Risk Indicators (KRIs) and Early Warning Indicators (EWIs) for emerging threats.
10. Formulate post-crisis recovery plans emphasizing accelerated restoration and organizational learning.
11. Address specific risks including cyber security events, data privacy breaches, and ESG-related operational crises.
12. Integrate BCM, DR, and Crisis Management into a single, cohesive resilience ecosystem.
13. Foster a proactive, risk-aware culture that links personal conduct to overall organizational stability.

Target Audience

1. Operational Risk Managers/Specialists
2. Heads of Business Continuity Management (BCM)
3. Chief Operating Officers (COO) and Senior Operations Leaders
4. Enterprise Risk Management (ERM) Professionals
5. Compliance and Governance Officers
6. Information Security and Cyber Resilience Managers
7. Internal Audit Professionals
8. Supply Chain and Vendor Risk Managers

Course Modules

Module 1: The New Operational Risk Landscape and Resilience Foundations

- Defining Operational Resilience and Business Continuity (BCM) and Disaster Recovery (DR).
- Basel Principles and regulatory expectations for Operational Risk Management (ORM).
- Mapping Critical Business Services and setting Impact Tolerances for Disruption.
- The interconnected nature of Cyber, Third-Party, and Conduct Risk.
- Case Study: The Global Cyber Extortion Event.

Module 2: Crisis Leadership and Decision-Making

- Establishing the Crisis Command Structure
- Real-time information gathering and rapid intelligence triage during an event.
- Structured decision models.
- The role of the leader in maintaining team composure and setting clear objectives.
- Case Study: The Rogue Trader Incident.

Module 3: Incident Response and Crisis Activation

- Developing and testing a robust Crisis Activation Protocol.
- The triage and containment phases of a severe operational failure.
- Implementing technical and non-technical mitigation strategies
- Integrating Early Warning Indicators and Key Control Indicators into the response.
- Case Study: The Payment Systems Failure.

Module 4: Strategic Crisis Communication

- Developing a transparent and timely communication strategy for different stakeholders
- Managing the narrative, fighting misinformation, and protecting brand reputation.
- Preparing for media scrutiny and conducting effective press statements and interviews.
- Internal communication: maintaining morale and providing clear direction.
- Case Study: The Product Recall Crisis.

Module 5: Third-Party and Supply Chain Resilience

- Identifying and mapping Tier 1 and Tier 2 vendor dependencies for critical services.
- Implementing contractual resilience clauses and service-level agreements for crisis scenarios.
- Strategies for rapid vendor replacement or manual bypass during a critical third-party failure.
- Governance and monitoring of Fourth-Party Risk exposure.
- Case Study: The Supply Chain Blockage.

Module 6: Post-Crisis Recovery and Organisational Learning

- The transition from Response to Recovery phase and restoring normal operations.
- Conducting Root Cause Analysis and developing effective corrective action plans.
- The After-Action Review.
- Integrating new insights into the Risk and Control Self-Assessment process.
- Case Study: The Data Center Fire.

Module 7: Scenario-Based Planning and Simulation

- Designing Severe but Plausible crisis scenarios
- Methods for Tabletop Exercises and full-scale Simulation Training.

- Developing Behavioral Metrics to evaluate CMT performance under stress.
- Techniques for injects and managing escalating crisis complexity during simulations.
- Case Study: The Digital Transformation Failure.

Module 8: The Future of Operational Risk and Crisis Response

- The impact of AI, Machine Learning, and Hyper-Automation on risk identification and control.
- Integrating ESG Risks into the operational risk framework.
- Future regulatory trends focusing on Operational Resilience Metrics and reporting.
- Strategies for talent management.
- Case Study: The AI-Driven Compliance Error.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com