JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Operational Loss Prevention and Mitigation Training Course

12 – 23 September 2027
Muscat

Operational Loss Prevention and Mitigation Training Course

Ref: 271_8804 **Date:** 12 – 23 September 2027 **Location:** Muscat **Fees:** 9900 GBP

Operational Loss Prevention and Mitigation is a 2-week training course for operations managers, business continuity leads and risk coordinators in manufacturing, logistics, healthcare and other service organisations, and it ends with an Operational Loss Reduction Plan. Unplanned downtime, supplier failures and avoidable human error now erode margins faster than most cost programmes can recover them. Jupiter Prime Training runs this course on operational loss prevention and mitigation for leaders responsible for everyday process reliability.

Why Operational Loss Prevention and Mitigation Matters Now

Lean inventories and single-source suppliers have made production lines and service desks fragile, so one late shipment or failed machine can halt output for days. Customers and contract partners now write penalties for missed service levels into agreements, and insurers ask for evidence of controls before renewing cover. At the same time, experienced staff are retiring and taking undocumented know-how with them. Organisations that analyse failures at process level fix causes once; those that react to each incident keep paying for the same breakdowns. The course applies the ISO 31000 risk management guidelines to processes, continuity and incident learning.

Who Gains Most from Operational Loss Prevention and Mitigation

- Operations leads who own throughput, quality and downtime across plants, warehouses or service centres
- Business continuity heads who define recovery priorities and maintain continuity arrangements
- Risk coordinators who run process risk assessments and track mitigation actions
- Supply chain leads who manage critical suppliers, logistics routes and inventory buffers
- Quality and HSE leads who investigate incidents and drive corrective action

A plant or service site that sends its operations, continuity and supply chain leads together gains most, because the loss reduction actions they agree cross all three areas.

Operational Loss Prevention and Mitigation Capabilities

Participants learn to trace losses to their process causes, design controls that people actually follow and keep critical activities running when suppliers or systems fail.

- Map critical processes and locate failure points with FMEA — operations and maintenance planners
- Apply root cause methods that separate system flaws from individual error — incident review boards
- Design preventive and detective controls with clear owners and evidence — site leadership and auditors
- Calculate the cost of loss events and weigh mitigation investment against it — finance and budget holders
- Build business impact analysis and recovery strategies for priority activities — continuity committees
- Specify supplier contingency options for single-source dependencies — procurement and supply chain heads

Key Operational Loss Prevention and Mitigation Terms

- FMEA — failure mode and effects analysis, a method that rates each way a process step can fail by severity, occurrence and detection.
- Root cause — the underlying condition that, if removed, prevents a failure from recurring rather than only addressing its symptom.
- Business impact analysis — an assessment of how disruption to each activity harms the organisation over time, used to set recovery priorities.
- Recovery time objective — the target time within which a disrupted activity must be restored to an acceptable level.
- Human reliability — the probability that people perform a task correctly, influenced by design, workload, training and environment.
- Single point of failure — a component, supplier or person whose failure alone stops a critical process.

Operational Loss Prevention and Mitigation Day by Day

Day 1: The Cost of Operational Failure

- ISO 31000 Applied To Processes — Framing Operational Exposures In Context
- Cost Of Poor Quality Model — Making Hidden Operational Losses Visible
- Loss Event Categories — Downtime, Waste, Rework, Penalties And Claims
- Manufacturing And Hospital Case Comparison — Contrasting Failure Consequences
- Current Loss Baseline — Setting A Starting Point For Reduction

Day 2: Process Mapping and Failure Points

- SIPOC And Swimlane Maps — Clarifying Handoffs Where Failures Occur
- Value Stream Mapping — Locating Bottlenecks And Buffer Weaknesses
- Critical Process Selection — Prioritising Where Analysis Effort Goes
- Single Point Of Failure Scan — Equipment, Systems, People And Suppliers
- Process Exposure Inventory — Recording Failure Points With Owners

Day 3: Failure Mode and Effects Analysis

- FMEA Worksheet Construction — Listing Failure Modes For Each Step
- Severity, Occurrence And Detection Scales — Rating Failure Modes Consistently
- Action Priority Logic — Choosing Which Failure Modes To Treat First
- Service FMEA For Logistics And Call Centres — Adapting The Method
- FMEA Review Cycles — Keeping Ratings Current After Changes

Day 4: Root Cause Investigation

- Five Whys Technique — Reaching Causes Beyond The First Answer
- Ishikawa Fishbone Diagrams — Structuring Causes Across Categories
- Fault Tree Analysis — Combining Conditions That Produce A Failure
- Timeline And Barrier Analysis — Reconstructing How An Incident Unfolded
- Causal Statement Writing — Producing Actionable Investigation Findings

Day 5: Human Error and Reliability

- Error Types — Slips, Lapses, Mistakes And Violations Distinguished
- Performance Shaping Factors — Workload, Fatigue, Design And Training
- Error-Proofing And Poka-Yoke — Designing Steps That Prevent Mistakes
- Procedure And Checklist Design — Making Correct Action The Easy Action
- Just Culture Principles — Encouraging Reporting Without Excusing Recklessness

Day 6: Control Design and Mitigation Options

- Hierarchy Of Controls — Eliminate, Substitute, Engineer, Administer, Protect
- Preventive Versus Detective Controls — Balancing Cost And Coverage
- Control Ownership And Evidence — Defining Who Checks What And How
- Mitigation Cost-Benefit Comparison — Ranking Options By Loss Avoided
- Risk Transfer Through Insurance And Contracts — Shifting Residual Exposure

Day 7: Supply Disruption and Supplier Dependencies

- Supplier Criticality Mapping — Identifying Single And Sole Sources
- Multi-Tier Visibility — Tracing Sub-Supplier And Logistics Dependencies
- Buffer Stock And Dual Sourcing Trade-Offs — Balancing Cost And Continuity
- Supplier Continuity Questionnaires — Testing Readiness Before Contracting
- Disruption Early Warning Signals — Monitoring Lead Times And Financial Health

Day 8: Business Continuity Arrangements

- Business Impact Analysis — Setting Recovery Priorities For Activities
- Recovery Time And Point Objectives — Defining Acceptable Downtime
- Continuity Strategy Options — Alternate Sites, Workarounds And Manual Fallbacks
- Continuity Plan Structure — Roles, Call Trees And Activation Criteria
- Exercise Design — Tabletop And Live Tests Of Recovery Arrangements

Day 9: Incident Learning and Monitoring

- Incident And Near-Miss Reporting Systems — Capturing Weak Signals Early
- Corrective And Preventive Action Tracking — Verifying Fixes Actually Work
- Leading Operational Indicators — Maintenance Backlog, Overtime And Rework
- Lessons Learned Reviews — Sharing Findings Across Sites And Shifts
- Loss Reduction Dashboard — Reporting Trends To Senior Leadership

Day 10: Practising the Operational Loss Reduction Plan

- Applying FMEA — Rating Failure Modes In A Case Distribution Centre
- Applying Root Cause Methods — Investigating A Recurring Production Stoppage
- Applying Business Impact Analysis — Prioritising Recovery For A Service Line
- Peer Review Panel — Challenging Mitigation Choices And Cost Estimates
- Operational Loss Reduction Plan — Sequencing Controls, Owners And Targets

Applying Operational Loss Prevention and Mitigation After the Course

- Lead an FMEA session on the process with the highest recent downtime and agree the three failure modes to treat first.
- Run a single point of failure scan of critical suppliers with procurement and present dual sourcing or buffer options to site leadership.

Operational Loss Prevention and Mitigation Questions FAQ

What is operational loss prevention and mitigation and why does it matter now?

Operational loss prevention and mitigation is the practice of finding where processes, people and suppliers fail and designing controls and recovery arrangements before losses occur. It matters now because lean supply chains and contractual penalties make every breakdown more expensive.

Which roles gain most from operational loss prevention and mitigation training?

Operations managers, business continuity leads and risk coordinators in industry and services gain most. Supply chain, quality and HSE leads who investigate incidents and manage critical suppliers also benefit from the shared methods.

How does operational loss prevention and mitigation differ from operational risk in banking?

Operational loss prevention and mitigation targets plants, logistics and service operations using FMEA, root cause analysis and continuity planning. Operational risk in banking centres on loss databases, capital calculation and supervisory resilience expectations specific to financial institutions.

What do you bring back from operational loss prevention and mitigation training?

You bring back a sequenced plan of controls, owners and loss reduction targets for your priority processes. It comes with FMEA worksheets, root cause templates and a business impact analysis format you can reuse across sites.

Operational Loss Prevention and Mitigation: The Way Forward

The Operational Loss Reduction Plan first informs which process failures receive mitigation budget in the next operating cycle. Operations and continuity leads use it with site leadership and finance to track losses avoided. After its first use, revisit the human reliability findings, because new procedures often shift error to steps nobody had examined before.