JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Supplier Network Resilience and Disruption Risk Training Course

26 April – 7 May 2027
Munich

Advanced Supplier Network Resilience and Disruption Risk Training Course

Ref: 453_16363 **Date:** 26 April – 7 May 2027 **Location:** Munich **Fees:** 9500 GBP

Supplier Network Resilience and Disruption Risk is an advanced 2-week training course for supply risk managers, sourcing leads and continuity planners, built around one work product: a Supplier Network Resilience Plan with a disruption risk register covering critical suppliers, their sub-tiers, recovery targets and mitigation options. Single points of failure deep in supplier networks now halt production and service faster than most organisations can react. Jupiter Prime Training designed this course for the people charged with seeing those failures coming.

Why Supplier Network Resilience and Disruption Risk Matter Now

Three forces push supplier resilience up the boardroom agenda. Geographic concentration of key components and materials means one port closure, extreme weather event or regional conflict can stop many buyers at once. Supplier insolvency rises when interest rates and input costs squeeze margins, often with little warning. And customers and insurers ask organisations to evidence how they would keep supplying after a disruption. Organisations that map and stress-test their supplier networks recover in days; those that discover their sub-tier dependencies during a crisis lose weeks and customers. The course draws on ISO 28000 security management systems for the supply chain and ISO 22301 business continuity management systems.

Who Gains Most from Supplier Network Resilience and Disruption Risk

- Specialists who identify and score risks across critical supplier relationships
- Sourcing leads who decide between single, dual and multiple sourcing
- Planners who set recovery time targets and continuity arrangements for supply
- Analysts who monitor supplier financial health and geographic exposure
- Coordinators who run disruption response and supplier communication during incidents

A cross-functional resilience cell from one organisation, combining sourcing, risk and continuity planning, gains most when its members attend together and agree one view of critical suppliers.

Supplier Network Resilience and Disruption Risk Capabilities

Each outcome replaces assumptions about suppliers with evidence about where the network would break and how fast it could recover.

- Map critical suppliers and their sub-tier dependencies for key products — sourcing strategy decisions
- Assess supplier financial distress signals and geographic concentration — risk committees
- Design disruption scenarios and estimate time-to-recover against time-to-survive — executive leadership
- Weigh buffer stock, dual sourcing and capacity reservation options — budget owners
- Specify recovery time objectives and continuity requirements for suppliers — supplier contracts
- Build a disruption risk register with owners, triggers and response actions — continuity planners

Key Supplier Network Resilience and Disruption Risk Terms

- Sub-tier supplier — a supplier to one of the organisation's direct suppliers, often invisible to the buyer until a disruption occurs.
- Time-to-recover — how long a supplier or site needs to restore full output after a disruptive event.
- Time-to-survive — how long the organisation can keep meeting demand from stock and alternatives before a disruption hits customers.
- Single point of failure — a supplier, site or route whose loss would stop supply because no qualified alternative exists.
- Dual sourcing — qualifying two suppliers for the same item so volume can shift if one is disrupted.
- Recovery time objective — the agreed maximum time within which a supply or activity must be restored after an incident.

Supplier Network Resilience and Disruption Risk Day by Day

Day 1: The Disruption Landscape

- Disruption Typology — Natural, Geopolitical, Financial and Cyber Events
- Supplier Concentration Indicators — Exposure From Shared Sources
- Resilience Versus Efficiency Trade-Off — Lean Inventory Consequences
- Stakeholder Expectations of Supply Continuity — Customers and Insurers
- Resilience Maturity Self-Assessment — Starting Priorities

Day 2: Mapping the Supplier Network

- Critical Item Identification — Revenue and Service Impact Ranking
- Sub-Tier Mapping Questionnaires — Visibility Beyond Direct Suppliers
- Supplier Site and Route Mapping — Geographic Hotspot Detection
- Bill of Materials Dependency Tracing — Shared Component Exposure
- Single Point of Failure Register — Alternative Source Gaps

Day 3: Supplier Risk Assessment Methods

- Supplier Risk Scoring Model — Likelihood and Impact Criteria
- Financial Distress Indicators — Liquidity and Payment Behaviour Signals
- Geographic and Political Exposure Scoring — Country-Neutral Hazard Factors
- Operational Capability Audits — Capacity and Quality Fragility
- Cyber and Information Risk in Suppliers — Access and Data Dependencies

Day 4: Security and Continuity Standards

- ISO 28000 Security Management Systems for the Supply Chain — Control Areas
- ISO 22301 Business Continuity Management Systems — Supply Continuity Applications
- Business Impact Analysis for Supply — Critical Activities and Dependencies
- Recovery Time Objectives for Suppliers — Setting Realistic Targets
- Supplier Continuity Plan Requests — Evidence to Demand

Day 5: Disruption Scenario Analysis

- Scenario Design Method — Plausible Severe Events
- Time-to-Recover Versus Time-to-Survive Comparison — Exposure Windows
- Stress Testing Supply Plans — Demand and Capacity Shocks
- Domino Effect Tracing — Knock-On Impacts Across Tiers
- Scenario Results Communication — Executive Risk Appetite Discussion

Day 6: Mitigation Strategy Options

- Buffer Stock Sizing — Strategic Inventory for Critical Items
- Dual and Multiple Sourcing — Qualification Cost Versus Protection
- Capacity Reservation Agreements — Priority Allocation Rights
- Nearshoring and Regional Sourcing Options — Lead Time and Cost Effects
- Design for Resilience — Component Standardisation and Substitution

Day 7: Contractual and Financial Protection

- Continuity Clauses in Supplier Contracts — Notification and Recovery Duties
- Supplier Financial Support Options — Early Payment and Tooling Ownership
- Insurance for Contingent Business Interruption — Cover Gaps
- Exit and Step-In Rights — Protecting Critical Supply
- Resilience Investment Business Case — Cost of Disruption Avoided

Day 8: Monitoring and Early Warning

- Supplier Risk Watchlist — Trigger Thresholds and Owners
- Early Warning Indicators — Delivery, Quality and Financial Signals
- Event Monitoring Routines — Weather, Port and Market Alerts
- Supplier Self-Reporting Requirements — Capacity and Incident Notices
- Risk Register Review Cadence — Updating Scores and Actions

Day 9: Responding to Disruption

- Supply Incident Response Team Roles — Command and Escalation
- Allocation Rules During Shortage — Customer and Product Priorities
- Alternative Supplier Activation Playbook — Qualification Fast-Track
- Stakeholder Communication During Disruption — Customers and Regulators
- Post-Incident Review — Lessons Into Risk Register Updates

Day 10: Practising the Supplier Network Resilience Plan

- Sub-Tier Mapping Exercise — Applying Dependency Tracing to a Product
- Risk Scoring Calibration — Applying the Supplier Risk Model to Cases
- Disruption Simulation — Applying Scenario Analysis and Response Roles
- Mitigation Selection Debate — Applying Buffer and Dual Sourcing Trade-Offs
- Supplier Network Resilience Plan — Risk Register, Recovery Targets and Actions

Applying Supplier Network Resilience and Disruption Risk After the Course

- Select the five most critical items and trace their sub-tier suppliers to list every single point of failure with a proposed mitigation.
- Run a time-to-recover versus time-to-survive comparison for the top ten suppliers and present the largest exposure windows to the risk committee.

Supplier Network Resilience and Disruption Risk Questions FAQ

What is supplier network resilience and disruption risk, and why does it matter now?

It is the practice of mapping supplier dependencies, scoring disruption risk and preparing mitigation and recovery before a crisis. It matters now because concentrated sources, supplier insolvency and extreme events can halt supply with little warning.

Which roles gain most from supplier network resilience and disruption risk training?

Supply risk managers, sourcing leads and continuity planners gain most. They decide which suppliers are critical, how risks are scored, which mitigations to fund and how the organisation responds when supply fails.

How does supplier network resilience and disruption risk training differ from a general business continuity course?

A general business continuity course covers all critical activities across an organisation. This course concentrates on supply: sub-tier mapping, supplier risk scoring, dual sourcing, buffer stock, supplier contracts and response to supply shortages.

What do you bring back from supplier network resilience and disruption risk training?

You bring back a resilience plan with a supplier dependency map, a risk scoring model, disruption scenarios, mitigation options, recovery time targets and a risk register ready to adopt.

Supplier Network Resilience and Disruption Risk: The Way Forward

The Supplier Network Resilience Plan first informs which critical items receive dual sourcing or buffer stock investment. Risk managers own the register, sourcing leads act on mitigations and continuity planners rehearse responses. After the first real disruption or simulation, revisit recovery targets and early warning triggers to see where detection or response was slower than planned.