

# Supplier Continuity Collaboration Outline

THIRD-PARTY RESILIENCE

DELIVERABLE Collaboration outline with tabletop prompts

## PURPOSE

Rehearse supplier incidents, align on dependencies, and keep recovery coordinated across functions.

## SCOPE & CONTEXT

TOPIC	DETAILS
Critical supplier	
Service dependency	
SLA / continuity target	
Existing mitigations	
Open issues / vulnerabilities	

## CONTINUITY REVIEW CHECKPOINTS

Use this section to guide the tabletop or review discussion:

- Confirm supplier health signals (performance, security, financial, delivery).
- Validate incident triggers (severity, impact, scope).
- Recheck escalation contacts and handoffs.
- Review communication protocols (internal + external).
- Decide on resilience actions (switch suppliers, patch, deploy workarounds).

## TABLETOP PROMPTS

### PROMPT 1 — SUPPLY CHAIN BREAK

*What stops us from pivoting to an alternate supplier in 4 hours? Who owns the next decision if the supplier misses a milestone? What contract clauses guide price negotiation or termination?*

### PROMPT 2 — SUPPLIER COMPROMISE

*What is our detection window for an upstream breach? How do we isolate supplier-accessed systems? What dependencies require stakeholder notification (clients, regulators, partners)?*

### PROMPT 3 — SUPPLIER OUTAGE RIPPLE

*Which downstream services degrade first? What manual workarounds keep customers supported? How do we communicate impact without causing panic?*

## RECOVERY COMMITMENTS

ACTION	OWNER	DUE	STATUS

## REFLECTION & READINESS

- Supplier governance cadence documented.
- Legal / contracting notes up to date.
- Communication plan rehearsed.
- Post-tabletop debrief scheduled (owner + date).

### **DORA NOTE — For EU entities and regulated financial services:**

The Digital Operational Resilience Act (EU) 2022/2554 requires that firms assess ICT risk across their supply chain. If DORA applies, ensure your tabletop exercise covers the specific scenarios in Articles 10–13: ICT-related incidents, threat-led penetration testing, and third-party concentration risk. Consult your legal or compliance team for jurisdiction-specific scoping.