THIRD-PARTY CONTINGENCY PLAN

Critical Vendor • Banking Sector • OSFI E-21 / Operational Resilience Aligned

Document Owner: _____ | Version: 1.0 | Date: _____

Financial Industry Focus	Senior-Led Delivery	ISO 22301 + OSFI Fluency

Downloadable Maxvia Associés Third-Party Contingency Plan template. This document is designed for regulated organizations seeking continuous, audit-ready resilience capability.

Quick Exposure Checklist

Use this checklist to quickly determine whether the organization can continue delivering the listed critical banking services if the vendor becomes unavailable.

Check	Item	Status
1	Workaround defined and documented for vendor outage	☐ Yes ☐ No ☐ Partial
2	Critical business services impacted are identified and prioritized	☐ Yes ☐ No ☐ Partial
3	Manual / alternate processing steps are executable (not theoretical)	☐ Yes ☐ No ☐ Partial
4	Internal roles and on-call coverage are defined for an outage	☐ Yes ☐ No ☐ Partial
5	Customer and regulator communication approach is pre-approved	☐ Yes ☐ No ☐ Partial
6	Vendor outage scenario has been tested in the last 12 months	☐ Yes ☐ No ☐ Partial
7	Evidence is stored and retrievable for audit / supervisory review	☐ Yes ☐ No ☐ Partial

1. Vendor Profile (Single Critical Vendor)

Field	Value	Field	Value
Vendor Legal Name	_____	**Services Provided**	_____
Vendor Primary Contact	_____	**Contacts (24/7 Escalation)**	_____
Internal Vendor Owner	_____	**BCM Owner**	_____
Critical Services Supported	_____	**Primary Systems/Interfaces**	_____
Contract Reference	_____	**Service Location / Region**	_____
Known 4th Parties (Subcontractors)	_____	**Data/Processing Dependencies**	_____

Outage Detection Method	_____	**Monitoring Tools / Alerts**	_____

2. Scope & Objective

This contingency plan documents the organization's workaround and recovery capabilities if the above critical third-party vendor becomes unavailable. It is designed for the banking sector and supports OSFI E-21 operational resilience expectations by demonstrating the ability to sustain critical services during third-party disruption.

3. Vendor Failure Scenarios

Scenario ID	Scenario	Trigger / Description	Detection / Indicators	Owner	Severity
S1	Full Service Outage	Vendor service unavailable; transactions/processing halted	Monitoring alerts; client errors; vendor status page	Vendor Manager	High
S2	Partial Degradation	Service available but degraded; timeouts; partial functionality	Error rate spikes; latency alarms; user reports	IT Operations	Medium
S3	Cyber Incident at Vendor	Vendor disables services due to cyber event; containment actions	Security intel; vendor advisories; abnormal behavior	CISO / Security	High
S4	Data Integrity Event	Data corruption or integrity concerns impacting banking operations	Reconciliation failures; mismatched outputs; audit logs	Operations Lead	High
S5	Fourth-Party Disruption	Vendor impacted by its own critical supplier failure	Vendor notification; industry outage; dependency alerts	Vendor Manager	Medium

4. Impact Assessment (Business / Customer / Regulatory)

Impact Area	Description	Critical Services Affected	Notes
Operational	_____	_____	_____
Financial	_____	_____	_____
Customer / Client	_____	_____	_____
Regulatory / Supervisory	_____	_____	_____
Reputational	_____	_____	_____

5. Contingency Strategies (Operate Without the Vendor)

Strategy	When to Use	Workaround Steps	Prerequisites	Owner	Estimated Time to Activate	Evidence to Retain
Internal Manual Workaround	Immediate outage / short-term continuity	Describe manual steps and controls	Access, forms, approvals, staff coverage	Operations Lead	__ hrs	Logs, approvals, reconciliation records
Alternate Vendor / Substitute Provider	Sustained outage / vendor failure	Activation, onboarding, routing, data mapping	Pre-negotiated contract, access, runbooks	Vendor Manager	__ days	Contract, onboarding checklist, cutover records
Service Prioritization / Degradation	To preserve critical services	Define what is maintained vs paused	Pre-approved service tiers, comms templates	BCM Lead	__ hrs	Decision record, comms artifacts

6. Recovery Execution Plan (Step-by-Step)

Step	Action	Owner	Target Time	Inputs / Tools	Output / Evidence	Status
1	Detect disruption and validate vendor outage	IT Operations	0–15 min	Monitoring, alerts	Incident ticket opened	☐

2	Activate contingency plan and notify internal stakeholders	BCM Lead	15–30 min	Call tree, Teams bridge	Activation log	☐
3	Select strategy (manual workaround / alternate vendor / prioritization)	Incident Lead	30–60 min	Decision criteria	Decision record	☐
4	Execute workaround and stabilize critical services	Ops + IT Leads	< __ hrs	Runbooks, forms	Service restored (minimum viable)	☐
5	Communicate status (customers, management, regulators as required)	Comms Lead	Hourly / as needed	Templates	Comms archive	☐
6	Operate in contingency mode; track performance and risk	Ops Lead	Ongoing	KPIs, logs	Operational log	☐
7	Return to normal operations once vendor recovers	IT Lead	As available	Cutback plan	Post-incident report	☐

7. Roles & Responsibilities (RACI)

Activity	BCM Lead	Vendor Manager	IT Operations	Operations Lead	Comms Lead	Risk/Compliance
Detect & validate outage	A	C	R	C	I	I
Activate plan / incident bridge	R	C	C	C	I	A

Vendor escalation & status management	C	R	C	I	I	A
Execute manual workaround	C	I	C	R	I	A
Customer communications	I	I	I	C	R	A
Regulatory/internal reporting	A	C	I	C	C	R
Post-incident review & improvements	R	C	C	C	I	A

8. Communication Plan

Audience	Trigger	Channel	Owner	Message / Key Points	Frequency	Evidence
Executive Management	Plan activation	Email / Call	BCM Lead	Situation, impact, decision, next update	30–60 min	Email trail / minutes
Operations & IT Teams	Outage confirmed	Teams / Bridge	Incident Lead	Actions required, roles, timelines	15–30 min	Bridge log
Customers / Clients	Service impact	Email / Status page	Comms Lead	What happened, what is affected, workaround, ETA	As needed	Comms archive
OSFI / Regulators (if required)	Material impact	Formal notice	Risk/Compliance	Impact summary, mitigations, next steps	Per requirement	Submission record
Vendor	Escalation	Phone / Ticket	Vendor Manager	Outage confirmation, root cause request, recovery updates	Hourly	Tickets / notes

9. Testing & Validation

This plan must be tested at least annually using vendor-outage scenarios. Testing must generate evidence suitable for audit / supervisory review.

Test Type	Scenario	Frequency	Participants	Success Criteria	Evidence Produced	Remediation Owner
Tabletop Exercise	S1/S3 vendor outage	Annual	BCM, IT, Ops, Vendor Mgmt	Workaround executed; comms sent	Exercise report, logs	BCM Lead
Walkthrough	Manual workaround	Semi-annual	Ops teams	Steps executable; controls applied	Checklist, sign-off	Ops Lead
Evidence Review	Documentation & evidence pack	Annual	Risk/Compliance	Evidence complete & retrievable	Evidence index	Risk/Compliance

10. Continuous Improvement

After each test or incident, update this plan, track remediation actions, and refresh stakeholder contact lists. Retain evidence and decisions for audit and supervisory review.