Continuity Hub • Field Quick Card

Vendor Incident Quick Card: The Three Transmission Paths & Dual-Clock BIA

Current version — Nov 1, 2026
Update history: continuityhub.org/supply-chain-cybersecurity/

THE SEAM BETWEEN CYBER AND CONTINUITY

Vendor cyber incidents sit on the seam between the cybersecurity team's third-party risk work (*asks if the vendor is secure*) and the continuity team's planning (*asks what the business does when the vendor stops*). Treating "vendor down" as one scenario plans for the direct outage and improvises the data and integrity crises.

1. THREE TRANSMISSION PATHS (IN RISING ORDER OF SUBTLETY)

1. Direct Path — OPERATION = SERVICE

The vendor's service **is the operation** (SaaS platform, logistics tracking/dispatch, payroll processor). Their downtime is your downtime. Recovery timing is heavily influenced by their external incident response.

Plan Prompt: Activate offline manual workarounds; isolate process bottlenecks; do not wait on vendor status page updates.

2. Data Path — BREACH OF YOUR DATA

Vendor is breached holding company data. Your incident begins inside theirs: statutory notification clocks, customer inquiries, and regulatory exposure running on your name while facts live on their servers.

Plan Prompt: Trigger legal/regulatory notification protocol; enforce contractual data-accounting demands; draft external comms early.

3. Integrity Path — COMPROMISED RETURN

Vendor recovers, service returns — but can what returned be trusted? Reconnecting a compromised supplier's integrations at full speed is how one company's incident becomes two. Plans almost never name this path.

Plan Prompt: Suspend API/VPN pipes; enforce formal sanitization proof; run staging verification before full restoration.

2. PRE-INCIDENT LEVERS: CONTRACTS AS CONTINUITY INSTRUMENTS

Contracts are continuity instruments, yet most are drafted as commercial boilerplate. Focus on operational survival levers:

Contract Lever	Operational Function in Disruption	Common Pitfall • Failure Mode
Incident Notification Window	Hours between vendor discovery and your phone call. Determines whether your continuity response starts early or late.	Vague terms ("promptly", "as soon as commercially feasible") delay notice by days while breach escalates.
Security Requirements with Evidence	Current objective assessments (independent audits, not self-attestations). Dictates incident likelihood.	Relying on self-reported questionnaires or expired compliance certificates.
Data-Return & Exit Assistance	Contractual guarantees on standard data formats, escrow, and transition support if supplier collapses.	Proprietary data formats and lack of exit clauses turn migration into a hostage negotiation.
Integration Suspension Rights	Explicit unilateral rights to sever connections during a breach without financial or contractual penalty.	Vendor claims breach of contract or uptime SLA penalties if client disconnects compromised APIs.
Service Credits (The Fallacy)	Contracts lavish attention on service credits, but they refund a subscription fee — not an operational shutdown.	Mistaking financial credit clauses for business continuity and disaster recovery coverage.

3. THE VENDOR-DOWN CONTINUITY PLAYBOOK ESSENTIALS

Manual Workaround Sheet

Document pen-and-paper, spreadsheet, or batch fallbacks. Manual workarounds exist for more SaaS dependencies than their owners think, and fewer than plans claim. Verify fallback capacity limits.

Decision Rights: Suspend & Restore

Assign clear authority to disconnect vendor integrations upon breach, and strict multi-stakeholder clearance criteria before restoring connections to verify vendor integrity.

Customer Comms for 3rd-Party Breach

Pre-approved messaging acknowledging vendor disruption without absorbing third-party liability. Direct, factual reassurance regarding customer data and operational continuity.

Named-Vendor Tabletop Exercise

Run tabletop exercises using the vendor's actual name rather than generic placeholders. Generic drills never surface the specific individual who actually knows how to run the workaround.

Continuity Hub • Field Quick Card

Dual-Clock BIA: Procurement Lead Time vs. Vendor Stated RTO

Current version — Nov 1, 2026
Update history: continuityhub.org/supply-chain-cybersecurity/

LEAD TIME: THE NUMBER THE BIA IS MISSING

Continuity planning measures recovery time for systems; supplier failure runs on **procurement time**. When a critical vendor fails — cyber or otherwise — the binding constraint is rarely technical. It is the lead time to a working alternative. A BIA carrying only the vendor's RTO has measured the optimistic half of the outage.

1. THE DUAL-CLOCK OPERATIONAL FRAMEWORK

CLOCK 1: Vendor Stated RTO — OPTIMISTIC

What it measures: How long the vendor claims recovery will take under standard contractual SLA or disaster recovery declarations.
Governing factor: Vendor's internal incident response capability, clean backup restoration, and forensic containment.
Flaw: If ransomware destroys vendor infrastructure or negotiations stall, Clock 1 resets to infinity.

CLOCK 2: Substitution Lead Time — BINDING CONSTRAINT

What it measures: How long complete vendor replacement takes if vendor recovery fails or supplier becomes insolvent.
Governing factor: Sourcing, contracting, data migration, re-integration, validation, and market queue constraints.
Reality: *This is the clock your business will actually use when the crisis escalates.*

2. FOUR COMPONENTS OF SUBSTITUTION LEAD TIME (CLOCK 2)

Lead-Time Stage	Operational Friction Points & Critical Dependencies	Planning Requirement
1. Sourcing & Contracting	RFP/selection, Master Services Agreement, security reviews, legal redlining, executive approval for a replacement vendor during an active crisis.	Pre-qualify secondary suppliers; maintain active vendor shortlist or standby contract.
2. Data Migration	Extracting data held by incumbent vendor. Format (structured JSON/SQL vs proprietary blob) and contract exit clauses determine whether data is accessible.	Require periodic data escrow or automated daily client-side data backups in open format.
3. Re-Integration & Testing	Building new API connections, rewriting webhooks, re-validating ETL pipelines, and user acceptance testing across internal systems.	Maintain modular integration middleware; document interface specs in advance.
4. Concentration Queue	Every other customer of the failed vendor attempts to switch to the same alternative in the same week, overwhelming alternative onboarding teams.	Size lead times for surge delays (add 200–400% queuing buffer for market-wide incidents).

3. OPERATIONAL SIZING RULES AGAINST CLOCK 2

Inventory Buffers

Size safety stock and supply buffers against **Clock 2 (Substitution Lead Time)**, not Clock 1. If replacement takes 4 weeks, a 3-day buffer guarantees 25 days of dead operational stoppage.

Manual Fallback Sizing

Verify manual procedures can scale across the entire substitution window. Manual logs that collapse after 48 hours fail when alternative procurement requires 14 business days.

Dual-Sourcing Triggers

Where Clock 2 exceeds Maximum Tolerable Period of Disruption (MTPD), active dual-sourcing is mandatory. Split volume (e.g. 70/30) to keep secondary pipes warm.

4. VENDOR CYBER OUTAGE TRIAGE CHECKLIST

Step	Action Item	Verification Gate	Sign-Off
Triage 1	Identify Transmission Path (Direct, Data, Integrity).	Path-specific response team mobilized (IT, Legal, Comms).	[ ] Lead
Triage 2	Audit Incident Notification Window & demand written facts.	Vendor confirms nature of incident and data scope in writing.	[ ] Legal
Triage 3	Exercise Integration Suspension Rights if integrity compromised.	APIs, VPNs, and SFTP pipes disconnected and logged.	[ ] CISO
Triage 4	Deploy manual workaround with named workaround owner.	Business function operational in degraded fallback mode.	[ ] Ops
Triage 5	Initiate Dual-Clock comparison; evaluate substitution trigger.	Decision documented if vendor recovery exceeds Clock 2 threshold.	[ ] BCP Exec