SECTION 1 • THREE-PATH TRANSMISSION CHECKLIST

A continuity program that treats "vendor down" as one scenario has planned for the direct outage and improvised data and integrity crises. Use this checklist upon any supplier ransomware or cyber notification to classify transmission vectors and invoke path-specific operational controls.

CRITICAL VENDOR INCIDENT INTAKE & TRIAGE LOG

Incident Name / ID:	*INC-VENDOR-2026-___*	**Date / Time of Vendor Notice:**	*2026-___-___ ___:___ UTC*
Vendor Name:	*[Named Critical Supplier]*	**Internal Business Owner:**	*[Operations / BCP Lead]*
Critical Service Provided:	*[SaaS / Logistics / Payroll / Hosting]*	**Vendor Tier Level:**	*[Tier 1 Critical / Tier 2 Core]*

TRANSMISSION PATH 1: DIRECT-PATH ASSESSMENT (SERVICE = OPERATION)

Diagnostic Criteria	Status	Operational Response Action
Is vendor service the direct operational engine (e.g. dispatch, payroll, primary SaaS)?	[ ] YES [ ] NO	If YES, declare internal operational outage immediately. Do not await vendor ETA.
Has vendor provided verified, evidence-backed initial recovery timeline?	[ ] YES [ ] NO	If NO, assume vendor Clock 1 is compromised; initiate Clock 2 lead-time tracking.
Is offline / manual workaround documented with assigned owner?	[ ] YES [ ] NO	Mobilize named workaround owner; activate degraded operational buffer.

TRANSMISSION PATH 2: DATA-PATH ASSESSMENT (BREACH HOLDING COMPANY DATA)

Diagnostic Criteria	Status	Operational Response Action
Does vendor host, process, or store sensitive, customer, employee, or financial data?	[ ] YES [ ] NO	Invoke Data Protection Protocol. Start internal legal/regulatory incident clock.
Has vendor verified whether exfiltration or unauthorized access occurred?	[ ] YES [ ] NO	Enforce contractual data-accounting demand. Require forensic evidence report.
Are statutory regulatory notification clocks running in your organization's name?	[ ] YES [ ] NO	Deploy pre-cleared customer communications; brief legal counsel and privacy lead.

TRANSMISSION PATH 3: INTEGRITY-PATH ASSESSMENT (COMPROMISED RECOVERY)

Diagnostic Criteria	Status	Operational Response Action
Are automated API, SFTP, database, or VPN pipes active between supplier and network?	[ ] YES [ ] NO	Immediately invoke Integration Suspension Rights. Sever all active pipes.
Has vendor declared "service restored" or "recovered" following ransomware event?	[ ] YES [ ] NO	**HOLD RECONNECTION:** Reconnecting at full speed turns 1 incident into 2.
Has independent forensic evidence confirmed complete threat eradication?	[ ] YES [ ] NO	Require proof of clean staging environment before authorizing API reconnection.

SECTION 2 • CONTRACT-AS-CONTINUITY AUDIT WORKSHEET

Contracts are continuity instruments, yet most are drafted as if they were not. Service credits refund a subscription fee, not a business shutdown. This worksheet audits critical supplier agreements for the five operational continuity clauses that decide whether you survive the day.

MASTER VENDOR CONTRACT CONTINUITY AUDIT LOG

Clause Category	Current Contract Language / Status	Continuity Vulnerability	Required Remediation Standard
1. Incident Notification Window	*Window: [____] Hours* *Trigger: Discovery vs. Confirmation*	Vague terms ("promptly") allow vendor to conceal incident for days, crippling response.	Strict window: ≤ 24h (or ≤ 12h for critical Tier 1) upon initial detection/suspicion of breach.
2. Security Requirements with Evidence	*Evidence on file: [ ] Audit [ ] None* *Assessment Date: 202___*	Self-attestations or questionnaires lack objective verification and expire quietly.	Annual independent third-party assessment report (SOC 2 Type II, ISO audit, certified pen-test).
3. Data-Return & Exit Assistance	*Format: [Structured / Proprietary]* *Assistance SLA: [____] Days*	Proprietary data formats and lack of exit cooperation turn departure into hostage crisis.	Guaranteed data return within 48h in open format (JSON, CSV, SQL); mandated migration support.
4. Integration Suspension Rights	*Unilateral Right: [ ] Yes [ ] No* *Penalty Risk: [ ] Yes [ ] No*	Contract imposes breach or fee penalties if client disconnects compromised integrations.	Explicit unilateral right to sever APIs/VPNs on security suspicion without breach or penalty.
5. Service Credits De-Prioritizer	*Max Credit: [____]% subscription* *Operational Relief: Zero*	Service credits reimburse minor software fees while outage causes catastrophic business loss.	De-prioritize credit negotiation; reallocate bargaining leverage to clauses 1–4 above.

CONTRACT CONTINUITY SCORING MATRIX (VENDOR: _____)

Evaluation Check	Score (0–2)	Scoring Criteria	Action Required
Notification Window ≤ 24h	*[ ]*	2 = Fixed ≤24h; 1 = Fixed ≤72h; 0 = Vague / undefined	[ ] Redline
Objective Security Evidence	*[ ]*	2 = Current annual 3rd-party report; 1 = Questionnaire; 0 = None	[ ] Demand Audit
Open Data Return & Exit SLA	*[ ]*	2 = Standard format + transition SLA; 1 = Data only; 0 = Hostage format	[ ] Add Exit Addendum
Unilateral Suspension Rights	*[ ]*	2 = Unilateral without penalty; 1 = Mutual consent; 0 = Penalty risk	[ ] Protect API Cut
Total Contract Continuity Score:	_____ **/ 8 Points** • *(≥7 = Resilient; 4–6 = Degraded; ≤3 = High Critical Risk / Hostage Threat)*		

SECTION 3A • VENDOR-DOWN PLAYBOOK FILL-INS: MANUAL WORKAROUNDS

Manual workarounds exist for more SaaS dependencies than their owners think, and fewer than their plans claim. This sheet documents the exact degraded operational procedure, physical/spreadsheet tools, capacity limits, and named workaround owner before an incident occurs.

MANUAL WORKAROUND SPECIFICATION SHEET

Failed Critical System:	*[e.g. Core SaaS / Dispatch / Payroll]*	**Incumbent Vendor:**	*[Named Vendor]*
Named Workaround Owner:	*[Specific Individual Name & Title]*	**Backup Owner:**	*[Specific Individual Name & Title]*
Direct Phone / Mobile:	*[24/7 Contact Number]*	**Workaround Activation Time:**	*≤ [____] Hours from Outage*

OPERATIONAL WORKFLOW: PRIMARY SAAS VS. DEGRADED MANUAL MODE

Core Function	Automated SaaS Procedure (Normal)	Degraded Manual Procedure (Offline)	Offline Tooling
Data Intake & Logging	Real-time API ingestion into vendor SaaS database.	*Log incoming requests into encrypted local standalone spreadsheet: `[Local_Intake_Template.xlsx]`*	Encrypted Local Excel / Pen & Paper
Transaction Processing	Automated routing, dispatching, or payroll calculation.	*Named workaround owner executes batch offline manual approvals via dual-signoff authorization sheet.*	Batch Offline Log / Printed Manifests
Customer Confirmation	Automated transactional SMS / email triggers.	*Staff transmit manual templated notices via independent corporate email / voice channels.*	Independent Mail Client / Landline
Reconciliation Staging	Real-time bi-directional database sync.	*Queue sequential transaction batch files with hash verification for post-restoration data re-entry.*	Sequential Batch Audit Folder

WORKAROUND CAPACITY LIMITS & DEGRADATION CEILINGS

Throughput Capacity Ceiling

Manual fallback can process approximately **[____]%** of normal transaction volume.
Maximum sustainable manual operating duration: **[____] Days / Hours** before backlog exceeds recovery capacity.

Staffing & Fatigue Thresholds

Required personnel to maintain manual fallback: **[____] Staff**.
Shift rotation schedule: **[____]-hour shifts** to prevent critical data entry errors during prolonged manual operations.

DATA RE-ENTRY & POST-OUTAGE CATCH-UP PROTOCOL

When vendor service is verified and restored, execute the re-entry queue to reconcile the manual backlog:

Step 1	**Freeze Manual Processing**	Close the active manual transaction log and calculate total backlog volume.
Step 2	**Dual Integrity Verification**	Verify no duplicate transactions or conflicting account numbers exist in the manual file.
Step 3	**Staged Sequential Re-Entry**	Inject manual batch records into restored SaaS in chronological batches; verify audit logs.

SECTION 3B • CUSTOMER COMMS & SUSPEND/RESTORE DECISION RIGHTS

When someone else's breach affects your customers, poor communication absorbs their liability. Pre-approved messaging preserves trust without premature admissions. Concurrently, strict decision rights govern who can sever connections and who holds authority to reconnect.

1. CUSTOMER COMMUNICATION TEMPLATE (THIRD-PARTY SUPPLIER BREACH)

Subject: Operational Service Update — Upstream Provider Disruption • [Organization Name]

Dear [Customer Name / Valued Client],

We are writing to inform you of a temporary operational disruption affecting our [Service Name / Delivery Schedule]. This issue originates from an unscheduled cybersecurity incident on the network of an independent third-party technology provider, [Vendor Name / "one of our upstream platform providers"].

What We Know: Upon notification, our security team immediately enacted operational continuity protocols and severed direct system connections with the affected provider to safeguard all internal data environments.

What We Are Doing: Our teams have activated pre-established manual continuity workarounds to process critical transactions. Core services remain operational in fallback mode, though you may experience [describe specific delay or delivery adjustment, e.g. extended processing windows of 4–6 hours].

Data Security: We are actively monitoring the provider's forensic investigations. We have not detected any unauthorized access to our core systems. We will provide formal updates as verified facts are confirmed.

For immediate operational assistance, contact [Continuity Operations Desk at Phone / Email].

2. SUSPEND-AND-RESTORE DECISION-RIGHTS AUTHORITY LOG

Decision Gate	Authorized Decision Role	Required Evidence / Threshold	Fallback Authority
1. Integration Severance (Cut APIs / VPN)	Chief Information Security Officer (CISO) or Lead Architect	Notice or suspicion of supplier breach / abnormal upstream traffic.	On-duty Incident Commander / Lead Infrastructure Engineer
2. Manual Workaround Activation	Operations Director / BCP Lead	Confirmed SaaS downtime ≥ 2 hours or vendor response failure.	Designated Named Workaround Owner
3. External Customer Notice Approval	Chief Executive Officer / General Counsel	Confirmation that customer services or data scopes are impacted.	VP of Communications + Privacy Officer
4. Restoration Authorization (Reconnect)	Joint Sign-Off: CISO + Operations Director	Independent forensic proof of clean vendor staging environment.	Executive Risk Committee Consensus

3. RECONNECTION SAFETY GATE CHECKLIST (INTEGRITY-PATH DEFENSE)

Integrity Verification Check	Status	Verified Artifact / Documentation
Has vendor provided written confirmation of threat actor eradication?	[ ] YES [ ] NO	*Artifact: Incident eradication report / third-party letter*
Have all integration credentials, API keys, and certificates been rotated?	[ ] YES [ ] NO	*Artifact: Secret rotation audit log*
Has initial reconnection been tested in an isolated sandbox / staging pipe?	[ ] YES [ ] NO	*Artifact: Sandbox traffic inspection sign-off*
Is real-time traffic anomaly detection monitoring active on restored pipe?	[ ] YES [ ] NO	*Artifact: SIEM / Network telemetry verification*

SECTION 4 • NAMED-VENDOR TABLETOP EXERCISE SCRIPT

Generic cyber tabletop exercises fail because they never surface the specific individual who actually knows how to run the manual workaround. This exercise script requires inserting the vendor's actual name and forces teams to resolve real operational friction across all three transmission paths.

TABLETOP SESSION METADATA & ROLES

Exercise Date:	*2026-___-___*	**Lead Facilitator:**	*[BCP / Risk Lead]*
Named Target Supplier:	*[Insert Actual Critical Vendor Name]*	**Target Service:**	*[Core SaaS / Payroll / Logistics]*
Key Participants:	*CISO, Operations Lead, Legal Counsel, Communications Lead, Workaround Owner*		

TABLETOP SCENARIO PROGRESSION & OPERATIONAL INJECTS

PHASE 1 (T+00:00) • Silent Outage & Discovery Direct Path Trigger

Inject: At 08:15 on a high-volume business day, internal staff report that [Named Vendor]'s portal is unreachable. API calls return 503 gateway errors. The vendor's status page displays "Operational". Rumors on industry feeds suggest [Named Vendor] was hit by LockBit ransomware overnight.
Friction Questions: How many hours do we wait before declaring an internal incident? Who calls [Named Vendor]? Does our contract stipulate a notification window, or are we checking social media?

PHASE 2 (T+03:30) • The Workaround Owner Dilemma Operational Reality Check

Inject: [Named Vendor] sends a brief statement: "Experiencing a security event. Systems offline indefinitely." The business must operate. The BCP plan says "switch to offline manual processing."
Friction Questions: *Who specifically knows how to run the manual workaround?* Call out their name right now. Do they have the offline templates? What happens after 24 hours of backlog volume?

PHASE 3 (T+12:00) • The Data Breach Spillover Data Path Trigger

Inject: Media reports that the attackers exfiltrated customer databases from [Named Vendor]. Customers are calling your support lines asking if their records were compromised. Regulatory clocks are ticking.
Friction Questions: Do we have contractual audit rights to demand data exfiltration scope? Who approves the customer communication template? Who files notice with regulators if facts live on their servers?

PHASE 4 (T+48:00) • The Poisoned Return Integrity Path Trigger

Inject: [Named Vendor] announces: "All systems restored. Please re-enable API integrations." Engineering wants to reconnect immediately to clear the manual backlog. However, no independent forensic audit report is provided.
Friction Questions: Who has the contractual and technical authority to say NO? What evidence is required before reconnecting? If we reconnect compromised pipes, who owns the secondary breach?

TABLETOP ACTION ITEM LOG & GAP TRACKER

Identified Gap	Corrective Action	Assigned Owner	Due Date
Workaround owner undefined	Formalize offline operating guide; designate primary & backup leads.	*[Ops Lead]*	*2026-___-___*
No contract suspension clause	Draft security addendum reserving unilateral API severance rights.	*[Legal Counsel]*	*2026-___-___*
Customer comms improvised	Pre-clear third-party breach customer messaging templates.	*[Comms Lead]*	*2026-___-___*

SECTION 5 • DUAL-CLOCK BIA WORKSHEET & LEAD-TIME CALCULATOR

A BIA that records the vendor's stated RTO but not replacement lead time has measured the optimistic half of the outage. Supplier failure runs on procurement time. Use this worksheet to calculate Clock 2 (Substitution Lead Time) and size operational buffers against the real crisis clock.

CRITICAL VENDOR DEPENDENCY PROFILE

Critical Vendor Name:	*[Named Critical Supplier]*	**MTPD for Function:**	*[____] Business Days / Hours*
Service Category:	*[SaaS / Logistics / Payroll]*	**CLOCK 1: Stated Vendor RTO:**	***[____] Hours** (Contract SLA)*

CLOCK 2 LEAD-TIME CALCULATOR (SUBSTITUTION BREAKDOWN)

Substitution Phase	Operational Friction & Dependency Factors	Baseline Days	Surge / Crisis Days
1. Sourcing & Contracting	Market search, RFP selection, legal review, contract execution, credit check for alternative supplier.	*[ ] Days*	*[ ] Days*
2. Data Migration	Extracting records from incumbent, schema transformation, format conversion (JSON/SQL), database upload.	*[ ] Days*	*[ ] Days*
3. Re-Integration & Testing	Re-architecting API endpoints, authentication setup, webhook configuration, user acceptance testing.	*[ ] Days*	*[ ] Days*
4. Concentration Queue	Delay caused by peer organizations all seeking alternative onboarding in the same week following vendor collapse.	*[ ] Days*	*[ ] Days*
TOTAL CLOCK 2 • SUBSTITUTION LEAD TIME:		**____ Days / Hours** • *(Real Crisis Outage Window)*	

OPERATIONAL SIZING DECISIONS (SIZED AGAINST CLOCK 2)

Inventory Buffer Sizing

Physical safety stock or resource buffer required to bridge substitution window:
`Buffer Units = Daily Burn Rate × Clock 2 Days`
Current Buffer Capacity: **[____] Days** • Gap: **[____] Days**

Manual Fallback Capacity Sizing

Manual operational procedures must sustain through full Clock 2 duration:
Manual Staff Hours Required: **[____] Hours**
Overtime / Temporary Staffing Budget: **$[____]**

DUAL-SOURCING ACTIVATION DECISION THRESHOLD

Evaluation Check	Calculated Metric	Strategic Continuity Mandate
Does Clock 2 exceed MTPD?	*[ ] YES [ ] NO*	If Clock 2 > MTPD, single-sourcing is fatal. **Active dual-sourcing is mandatory.** Split live volume (e.g. 70/30) to maintain warm standby.
Is Data Migration > 48 hours?	*[ ] YES [ ] NO*	Implement automated daily offsite client-controlled backups in open JSON/CSV format immediately.

SIGN-OFF & CONTINUITY REVIEW RECORD

BCP Lead Sign-Off: _____ Date: _____	**CISO Sign-Off:** _____ Date: _____	**Executive Sponsor:** _____ Date: _____