Current version — Nov 1, 2026
Update history: continuityhub.org/controlled-relaunch-what-it-requires/

CONTROLLED RELAUNCH MASTER CHECKLIST: 7 GATES TO REOPEN

Operational workbook for operators and managers of customer-facing online ordering and delivery services recovering from an extended outage. Grounded strictly in Post 633.

RELAUNCH GOVERNING CHARTER
A controlled relaunch is a staged, verified, reversible return to service — not a single moment when everything switches back on. Functions return in a deliberate order, each stage opens only when its checks pass, and every stage carries pre-agreed conditions under which it closes again.

MASTER 7-GATE EXECUTION REGISTER

Gate	Relaunch Core Gate	Mandatory Verification Standard (Post 633)	Gate Owner	Sign-Off / Status
G-1	**Data Clean Proof**	Catalog, prices, inventory, accounts, in-flight orders audited against trusted state. Incident window quarantined.	Lead Data Architect	[ ] PASS / [ ] HOLD Date: _____
G-2	**Access Re-Credentialing**	Passwords, keys, tokens rotated; service accounts audited; vendor access granted on purpose; dormant accounts off.	Security Lead	[ ] PASS / [ ] HOLD Date: _____
G-3	**Staged Re-Entry**	Informational before transactions; one region/banner first; read-only before write. Gated on stability, not calendar.	Operations Director	[ ] PASS / [ ] HOLD Date: _____
G-4	**Physical Reconciliation**	Physical counted stock, warehouse flows, and scarce-item allocation match system before ordering unlocks.	Supply Chain Lead	[ ] PASS / [ ] HOLD Date: _____
G-5	**Sequenced Comms**	Phone/chat support briefed before channel reopens; refunds/credits pre-decided; staged customer announcements.	Comms & Support Lead	[ ] PASS / [ ] HOLD Date: _____
G-6	**Fraud Watchdog**	Heightened watch: lower transaction limits, anomaly review, fast freeze paths. Relax on evidence over days.	Fraud & Risk Lead	[ ] PASS / [ ] HOLD Date: _____
G-7	**Rollback Authority**	Pre-agreed written error/integrity/support volume criteria + single named shut-off authority without a meeting.	Incident Commander	[ ] PASS / [ ] HOLD Date: _____

INCIDENT METADATA & GOVERNANCE AUTHORIZATION

Incident Reference / Ticket:	_____	**Outage Duration (Days/Hours):**	_____
Customer-Facing Banners:	_____	**Pilot Reopen Region / Scope:**	_____
Incident Commander (Named):	_____	**Rollback Authority (Named):**	_____

The Core Warning (Post 633): Reopening on unverified data converts a systems outage into a correctness outage — in which customers are charged wrong prices, promised stock that does not exist, and shown information that is not theirs. Reopening against phantom inventory manufactures a second, self-inflicted outage. An operator who cannot state exact evidence thresholds for closing has only scheduled the announcement.

GATE 1: DATA VERIFICATION WORKSHEET & QUARANTINE LOG

Mandate: Before ordering reopens, data the service runs on must be verified against a state you trust. Transactions written during the incident window are reconciled or quarantined, not assumed good.

CORE DOMAIN VERIFICATION AUDIT

Data Domain	Verification Method & Trusted Baseline	Integrity Test	Findings / Discrepancies	Sign-Off
1. Product Catalog	Compare item master database against pre-incident trusted backup snapshot.	SKU count check; zero rogue/modified items.	[ ] Matched [ ] Altered: ____	Sign: _____ Date: _____
2. Price Tables & Rules	Audit active base prices, promos, tax tables against signed pre-incident price book.	Zero price anomalies; currency & discount rule audit.	[ ] Matched [ ] Altered: ____	Sign: _____ Date: _____
3. Inventory Records	Freeze inventory ledger. Reconcile system quantities against verified physical floor counts.	Variance audit; zero unverified phantom quantities.	[ ] Matched [ ] Altered: ____	Sign: _____ Date: _____
4. Customer Accounts	Audit user authentication states, stored profiles, addresses, balances, loyalty credits.	Zero record leakage; verify customer boundary isolation.	[ ] Matched [ ] Altered: ____	Sign: _____ Date: _____
5. In-Flight Orders	Extract all orders received/written during incident window. Reconcile or quarantine.	Payment capture audit; fulfillment state verification.	[ ] Matched [ ] Altered: ____	Sign: _____ Date: _____

INCIDENT WINDOW: RECONCILE OR QUARANTINE ACTION LOG

Order / Record ID	Timestamp Range	Transaction Description & Customer	Verification Finding	Action Taken	Authority Signature
#_____	___/___ __:__	_____	[ ] Verified Clean [ ] Corrupt / Unclear	[ ] Reconciled [ ] Quarantined	_____
#_____	___/___ __:__	_____	[ ] Verified Clean [ ] Corrupt / Unclear	[ ] Reconciled [ ] Quarantined	_____
#_____	___/___ __:__	_____	[ ] Verified Clean [ ] Corrupt / Unclear	[ ] Reconciled [ ] Quarantined	_____
#_____	___/___ __:__	_____	[ ] Verified Clean [ ] Corrupt / Unclear	[ ] Reconciled [ ] Quarantined	_____
#_____	___/___ __:__	_____	[ ] Verified Clean [ ] Corrupt / Unclear	[ ] Reconciled [ ] Quarantined	_____

Gate 1 Decision Standard: If ANY core domain or in-flight transaction cohort cannot be reconciled against a trusted state, it MUST be quarantined immediately. Relaunching on unverified data converts a systems outage into a correctness outage.

Current version — Nov 1, 2026
Update history: continuityhub.org/controlled-relaunch-what-it-requires/

GATE 2: ACCESS RE-CREDENTIALING INVENTORY SHEET

Mandate: A relaunch re-credentials access deliberately. Whatever path an incident used, it authenticated as something. Reopening with pre-incident credentials leaves every one of those doors exactly as it was found.

1. PASSWORDS, API KEYS & SESSION TOKENS (ROTATION REGISTER)

System / Surface	Credential Class	Rotation / Invalidation Method	Revocation Time	Verified By
Admin Portals & IAM	Admin/operator passwords & MFA secrets	Forced password reset; revoke all sessions	___/___ __:__	_____
API & Gateway Keys	External/internal REST API keys & tokens	Regenerate secrets; invalidate pre-incident tokens	___/___ __:__	_____
Database Credentials	Application database user passwords/certs	Rotate DB secrets; restart pool connections	___/___ __:__	_____
Customer Sessions	Web and mobile app JWTs / cookies	Global session invalidation; force clean re-login	___/___ __:__	_____

2. SERVICE ACCOUNTS INVENTORY & PRUNING

Service Account Name	Assigned Workload / Service	Privilege Scope Review	Credential Rotated	Sign-Off
svc-_____	Ordering / Catalog Sync	[ ] Least-privilege verified • [ ] Rights pruned	[ ] YES • Date: ___	_____
svc-_____	Payment Gateway Processor	[ ] Least-privilege verified • [ ] Rights pruned	[ ] YES • Date: ___	_____
svc-_____	Fulfillment & Warehouse Dispatch	[ ] Least-privilege verified • [ ] Rights pruned	[ ] YES • Date: ___	_____

3. THIRD-PARTY / VENDOR ACCESS (GRANTED ON PURPOSE) & DORMANT DISABLES

Vendor Access: Explicit Purpose Log

Vendor / Partner	Business Justification	Granted on Purpose?
Logistics / 3PL API	Order dispatch	[ ] YES — Sign: _____
Payment Gateway	Checkout settlement	[ ] YES — Sign: _____
Analytics / Marketing	Traffic monitoring	[ ] HELD DARK / [ ] YES

Dormant Accounts: Disable Log

Account Category	Inactivity Threshold	Disabled Immediately?
Dormant Employees	>30 days no login	[ ] DISABLED — Sign: ___
Former Contractors	Engagement closed	[ ] DISABLED — Sign: ___
Test / Staging Users	Non-production accounts	[ ] DISABLED — Sign: ___

GATE 3: STAGED RE-ENTRY GATE PLANNER

Mandate: Staged re-entry orders the return by risk and by need. Each stage is a gate, not a schedule — the next stage opens when the current one is demonstrably stable, not when the calendar says so. Keeping channels dark on purpose keeps blast radius controllable.

1. RISK & NEED HIERARCHY EXECUTION LADDER

Stage	Relaunch Scope	Specific Operational Capabilities	Stability Criteria (Before Advance)	Gate Status
Stage 0 (Dark Base)	Internal-Only Operational Verification	Admin networks, core database replication, warehouse intranet. No public exposure.	Data clean verified (Gate 1); credentials reset (Gate 2).	[ ] Complete Sign: _____
Stage 1 (Info-Only)	Informational Pages Before Transactions	Homepage, service status banner, FAQ, support policy, store locator. Zero cart/ordering.	CDN/web traffic stable, zero origin errors, support queue normal.	[ ] Complete Sign: _____
Stage 2 (Read-Only)	Read-Only Access Before Write Access	Catalog browsing, item search, store pricing check. Checkout & account updates disabled.	Catalog query latency <200ms; zero data corruption alerts.	[ ] Complete Sign: _____
Stage 3 (Pilot Scope)	One Region or Banner Before Whole Estate	Single pilot geography or single brand banner. Controlled customer order intake.	Payment settlement clean, warehouse pick rate 100%, errors zero.	[ ] Complete Sign: _____
Stage 4 (General)	Controlled General Service Return	Broader estate reopen under heightened monitoring. Secondary channels remain dark.	All 7 gates stable across multi-hour observation window.	[ ] Complete Sign: _____

2. DELIBERATE DARK CHANNELS REGISTER

Keeping some channels dark on purpose is not failure. It is how a relaunch stays small enough to control while the highest-need services come back first.

Channel / Capability	Deliberate Dark Justification	Reopening Trigger Condition	Current Dark Status
Bulk / B2B Commercial Ordering	Protect scarce stock; prevent single-buyer warehouse clearing.	Retail channel stable >72h + stock verified.	[ ] DELIBERATELY DARK
Third-Party Delivery Aggregators	Aggregator API surges risk overwhelming inventory feeds.	Direct brand app and web order flow proven.	[ ] DELIBERATELY DARK
Promotional Codes & Flash Sales	Eliminate price engine calculation load and coupon abuse.	Pricing reconciliation complete >48h.	[ ] DELIBERATELY DARK
Non-Essential Account Edits	Limit write paths to checkout transactions only.	Core payment settlement clean.	[ ] DELIBERATELY DARK

Current version — Nov 1, 2026
Update history: continuityhub.org/controlled-relaunch-what-it-requires/

GATE 4: PHYSICAL REALITY RECONCILIATION SHEET

Mandate: Digital systems hold a picture of the physical world — stock on shelves, goods in warehouses, deliveries in transit — and a long outage makes that picture stale. An operator who reopens ordering against phantom inventory manufactures a second, self-inflicted outage.

1. PHYSICAL COUNT VS. SYSTEM INVENTORY AUDIT

Warehouse / Location	Product Category / Line	Physical Counted Stock	System Stale Level	Variance	Reconciled?
Distribution Center 1	High-Velocity Core Essentials	_____ units	_____ units	_____ %	[ ] RECONCILED
Distribution Center 2	Fresh & Perishable Lines	_____ units	_____ units	_____ %	[ ] RECONCILED
Store Hub (Fulfillment)	Shelf Stock for Delivery	_____ units	_____ units	_____ %	[ ] RECONCILED

2. CONFIRMED DISTRIBUTION FLOWS & LOGISTICS CHECK

Logistics Component	Verification Requirement	Operational Reality	Confirmed?
Inbound Supply to Warehouses	Supplier shipments receiving into DC without manual backlog.	Receiving docks cleared; EDI functional.	[ ] YES • Sign: ___
Trunking / Middle-Mile	Truck routes from DCs to local fulfillment hubs operational.	Driver routes scheduled & GPS confirmed.	[ ] YES • Sign: ___
Last-Mile Delivery Fleets	Delivery vans, dispatch routing, and drivers ready for dispatch.	Capacity matched to stage order cap.	[ ] YES • Sign: ___

3. SCARCE-ITEM ALLOCATION RULES VS. PHANTOM INVENTORY PREVENTION

Scarce-Item Allocation Rules:

- Set hard purchase limits per customer account on high-demand essentials.
- Buffer safety stock (withhold 15–20% of system count from online availability).
- Throttle cart reservations (expire unpaid carts after 10 minutes).

The Phantom Inventory Threat:
Thousands of accepted orders that cannot be filled, each one a refund, an apology, and a story.
Rule: If stock is not physically confirmed on the shelf or pallet, it is zero in the ordering engine.

Current version — Nov 1, 2026
Update history: continuityhub.org/controlled-relaunch-what-it-requires/

GATE 5: SEQUENCED COMMUNICATION SCRIPT & BRIEFING SHEET

Mandate: Communication in a relaunch is sequenced, not improvised. What is known is said early; reopening is announced stage by stage rather than promised whole; frontline support is briefed before each channel reopens; refund decisions are pre-made.

1. COMMUNICATION SEQUENCING PROTOCOL

Sequence	Recipient Group	Mandatory Content & Protocol	Timing Rule	Sign-Off
Step 1	**Phones & Chat Support**	Provide complete briefing package: what reopens, what stays dark, exact refund/credit policy, error escalation path.	BEFORE channel opens (never after).	[ ] Briefed Sign: ____
Step 2	**Pending Incident Customers**	Direct update to customers who had orders in flight: explicit status, refund confirmation or re-order schedule.	Preceding public announcement.	[ ] Sent Sign: ____
Step 3	**Public / App Announcements**	Stage-by-stage status announcement (e.g. pilot banner active, limited slots). Say what is known; do not promise all at once.	Synchronized with Gate 3 re-entry.	[ ] Published Sign: ____

2. PRE-DECIDED UNFULFILLED ORDERS, REFUNDS & CREDITS DECISION LOG

Decisions made before the first stage opens, so the answer a customer gets does not depend on which employee they happen to reach.

Customer Order Scenario	Pre-Decided Policy Answer (Uniform Across All Channels)	Processing SLA	Approved By
Order Placed Before Outage (Unfulfilled)	Automatic full refund to original payment method + apology credit issued. Customer does not need to submit request.	Within 24–48 hours	Finance & CX
Charged During Outage Window	Payment reversed immediately. Account credited with courtesy balance. Transaction logged in quarantine ledger.	Immediate / 24h	Finance & CX
Subscription / Delivery Pass Active	Pro-rata extension added automatically for full duration of outage plus courtesy grace period.	Batch automated	Finance & CX

3. STANDARD FRONTLINE SUPPORT SCRIPT (VERBATIM)

Customer Query: *"Can I order right now, and what happened to my previous order?"*
Uniform Staff Response: *"We are in a controlled relaunch of our delivery service. We are reopening stage by stage to ensure every order is fulfilled accurately. Any order placed prior to the outage that could not be delivered has been automatically refunded in full. New delivery slots are reopening progressively for [Pilot Banner/Region]. Thank you for your patience while we bring systems back safely."*

Current version — Nov 1, 2026
Update history: continuityhub.org/controlled-relaunch-what-it-requires/

GATES 6 & 7: HEIGHTENED FRAUD WATCH & ROLLBACK TRIGGER CARD

GATE 6: REOPENED-CHANNEL FRAUD WATCH CARD

Mandate: A reopened channel is a target. The days after a public outage are when stolen credentials get tested, payment fraud gets attempted, and ATO traffic arrives dressed as returning customers.

Fraud Watch Control	Heightened Relaunch Threshold	Relaxation Requirement (Evidence-Based)
Transaction & Order Limits	Temporary order cap ($150 / 2 orders per account/day) to prevent automated bulk basket drains.	Relax over days based on clean chargeback & settlement evidence — never on day one.
Anomaly & ATO Review	Strict velocity rules: flag rapid password changes followed by high-ticket orders; flag IP mismatches.	Manual review team embedded in relaunch crew; daily audit log of flagged vs legitimate logins.
Fast Freeze Paths	One-click automated payment authorization freeze for any checkout surge exceeding 3x baseline.	Maintained active through all staged re-entry phases until general release stability proven.

GATE 7: PRE-AGREED ROLLBACK CRITERIA & NAMED SHUT-OFF AUTHORITY

Mandate: Every stage carries rollback criteria written down in advance — and ONE named person with the authority to make that call without convening a meeting.

Rollback Trigger Metric	Explicit Numerical / Operational Threshold	Mandatory Rollback Action
1. System Error Rates	Checkout API error rate >1.5% over 10 minutes OR database replication lag >30 seconds.	Close checkout immediately; return site to Read-Only informational stage.
2. Data Integrity Anomalies	ANY instance of incorrect price charged, mismatched customer data displayed, or negative inventory.	Immediate halt to new order intake; quarantine all transactions in current window.
3. Support Volume Spikes	Customer contact center queue on order errors >25 calls/hour or unassigned chat wait >10 min.	Freeze ordering intake slots; divert traffic to status notice.

NAMED SHUT-OFF AUTHORITY (NO MEETING REQUIRED)

By charter of this controlled relaunch, the individual named below possesses sole, unilateral authority to execute immediate rollback of any or all relaunch stages upon breach of any trigger above, without convening a committee, consultation, or executive meeting.

Designated Shut-Off Authority:	Name: _____	Title: Incident Commander / Lead Operator
Direct Emergency Channel / Phone:	_____	**Backup Authority:** _____
Authority Signature:	_____	**Date & Time Authorized:** ___/___ __:__