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

CONTROLLED RELAUNCH QUICK CARD: 7 REOPENING GATES

Governing standard for returning customer-facing online ordering or delivery services after extended outage. Grounded strictly in Post 633.

WHAT "CONTROLLED" MEANS IN A CONTROLLED RELAUNCH

FUNDAMENTAL PRINCIPLE

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.

The Uncontrolled Relaunch (Failure Mode): Restore systems, reopen every channel at once, and discover remaining problems in public, at full volume, in front of every customer at the same time.

STAGE I: DATA & ACCESS TRUST ARCHITECTURE

GATE 1 Can you prove the data is clean before the first order?

DATA VERIFICATION GATE

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 Standard (Post 633)	Risk of Unverified Reopening
Product Catalog	Item definitions, active SKUs, and listings matched to trusted pre-incident state.	Showing corrupt, missing, or altered item listings.
Pricing Rules	Base prices, promotional rules, and currency verified; no unverified modifications.	Customers charged incorrect prices (hard to detect, destroys trust).
Inventory Levels	System counts frozen and audited against physical reality before allowing orders.	Promising stock that does not exist; massive unfilled orders.
Customer Accounts	Balances, profiles, loyalty records, and authentication states verified intact.	Showing customers information that is not theirs (privacy violation).
In-Flight Orders	Orders created during incident window segregated: reconciled or quarantined.	Duplicate fulfillment, lost charges, or unrecorded customer debt.

Correctness Outage Warning: Reopening on unverified data converts a systems outage into a correctness outage — failures that are slower to detect and harder to forgive than downtime.

GATE 2 Whose credentials still work — and whose should not?

ACCESS RE-CREDENTIALING GATE

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.

Credential Category	Mandatory Action Before Relaunch
Pre-Incident Passwords, Keys & Tokens	All pre-incident passwords, API keys, session tokens rotated or re-issued.
Service Accounts	Complete inventory conducted; rights pruned; credentials replaced.

Access Category	Mandatory Action Before Relaunch
Third-Party & Vendor Access	Granted again on purpose; zero inherited default vendor access.
Dormant Accounts	Disabled immediately; not left for post-relaunch clean-up.

STAGE II: STAGED RE-ENTRY & PERIMETER BOUNDARY

GATE 3 What reopens first — and what deliberately stays dark?

STAGED RE-ENTRY GATE

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 the blast radius controllable while highest-need services return first.

Order of Return (Risk & Need Hierarchy):

- **1. Informational pages before transactions** (status, browse, FAQ first).
- **2. One region or banner before the whole estate** (isolated blast radius).
- **3. Read-only access before write access** (catalog search before checkout).

Deliberate Dark Channels Policy:

- Keep secondary sales channels, batch bulk orders, and third-party feeds dark.
- Gate transitions on demonstrated system and operational stability.
- Never advance a stage because of calendar dates or public pressure.

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

CONTROLLED RELAUNCH QUICK CARD: GATES 4 – 7 & SIGN-OFF MATRIX

STAGE III: PHYSICAL REALITY, COMMUNICATIONS & CHANNEL DEFENSE

GATE 4 Does the physical operation match what the system believes?

PHYSICAL RECONCILIATION GATE

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.

Physical Truth Verification:

- **Counted Stock:** Physical floor counts at distribution centers before inventory feeds unlock.
- **Confirmed Distribution Flows:** Trunking, sorting, and last-mile carrier availability verified operational.
- **Scarce-Item Allocation:** Allocation rules configured to prevent immediate stockout runs.

The Phantom Inventory Threat:
An operator who reopens ordering against phantom inventory manufactures a second, self-inflicted outage: thousands of accepted orders that cannot be filled, each one a refund, an apology, and a story.

GATE 5 What do customers hear, and in what order?

SEQUENCED COMMS GATE

Communication in a relaunch is sequenced, not improvised. The first message matters as much as the first transaction: it confirms the service is run carefully or the opposite.

Audience / Sequence	Mandatory Briefing & Message Rule	Operational Principle
Frontline Support (Phones & Chat)	Briefed BEFORE each channel reopens, not after customers discover it.	Frontline carries pre-decided answers; no guessing.
Unfulfilled Orders, Refunds & Credits	Decisions made before the first stage opens; uniform policy across channels.	Customer answer does not depend on who they reach.
Public & Customer Announcements	What is known is said early; reopening announced stage by stage, never whole.	Confirm deliberate care; do not promise all at once.

GATE 6 Who is watching the reopened channel for fraud?

FRAUD WATCHDOG GATE

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

Heightened Fraud Controls:

- **Lower Transaction Limits:** Temporary order caps to curb bulk illicit drains.
- **Closer Anomaly Review:** Heightened velocity and IP/address deviation scoring.
- **Faster Freeze Paths:** Rapid account hold mechanisms for suspicious surges.

Team & Relaxation Standard:

- Treat monitoring team as part of the relaunch crew, not an audience.
- Controls relax on evidence, over days, not on the first quiet morning.
- Daily evidence log required before any limit increment.

STAGE IV: ROLLBACK DISCIPLINE & MASTER GATE SIGN-OFF

GATE 7 What would make you turn it off again?

ROLLBACK AUTHORITY GATE

Every stage carries rollback criteria written down in advance: the error rates, integrity anomalies, or support volumes that mean close it again — and **one named person with the authority to make that call without convening a meeting**.

This criterion separates a plan from a hope. An operator who cannot state exact evidence thresholds and name the single shut-off authority has only scheduled the announcement.

Pre-Written Rollback Metric	Trigger Threshold (Defined Before Launch)	Shut-Off Mechanism
Error Rates	API 5xx errors, checkout failures, or cart sync dropouts exceeding threshold.	Immediate return to read-only or dark channel state.
Integrity Anomalies	Price discrepancy, inventory negative drift, or mismatched customer record.	Transaction intake halt; quarantine log activated.
Support Volume Spikes	Contact center queue breach on order failure / wrong charging inquiries.	Stage intake freeze; support recovery script invoked.

THE SHORT VERSION: 7-GATE RELAUNCH VERIFICATION RECORD

Gate	Relaunch Core Gate	Verification Criterion (Post 633)	Status	Sign-off
G-1	Data Clean Proof	Catalog, prices, inventory, accounts, in-flight verified clean	[ ] PASS	_____
G-2	Access Re-credentialing	Passwords/keys rotated, service accounts checked, dormant off	[ ] PASS	_____
G-3	Staged Re-entry	Info before transaction, one region/banner, stability gates	[ ] PASS	_____
G-4	Physical Reconciliation	Counted stock, distribution flows confirmed, phantom avoided	[ ] PASS	_____
G-5	Sequenced Comms	Frontline briefed first, refund policy fixed, stage updates	[ ] PASS	_____
G-6	Fraud Watchdog	Lower limits, anomaly review, fast freezes, active crew	[ ] PASS	_____
G-7	Rollback Authority	Written error/integrity triggers + single named shut-off authority	[ ] PASS	_____