

USE CASE 06 / COTO PPT 137

Actionable supply-chain communications

Proposed operating design, version 2.0, 28 October 2026. Source concepts are from the COTO presentation; detailed controls, timelines, test gates and charging units are implementation proposals, not PPT quotations or live-service promises. All examples are synthetic. Prices and trade principal remain USD; local labour payments follow mandatory local rules. No invented partners, committed customers, tariffs or efficiency results are asserted.

Business outcome

Turn a reliable event into a clear assigned action, with acknowledgement and escalation rather than a stream of unverified messages.

Accountable roles

An operations coordinator owns the exception queue; each event source attests its facts; the designated recipient accepts an action. Business representatives alone approve changes to contractual commitments.

Required information

Order/lot and event IDs; source and source time; observed versus estimated status; freshness limit; affected site/quantity/date; recipient roles and agreed channel/consent; required action; due time/time zone; escalation owner; confidentiality classification.

Separate lifecycle states

Event: received > validated > routed. Action: open > notified > acknowledged > action-complete > reviewed/closed. Delivery failed, stale-source, overdue and disputed are explicit exception states. Notification delivered does not mean goods delivered or action accepted.

THE OPERATING WORKFLOW

From a real input to an approved outcome

01 / Define the event-to-action rules

Responsible: Coordinator + trading parties

Start with five events: approval needed, dispatch change, receipt mismatch, invoice due and quality concern. For each, define source, intended recipient, allowed fields, due time and escalation. Timing targets are pilot configuration, not a universal SLA.

02 / Validate source and freshness

Responsible: Rules + source owner

Require the matching order and permitted actor. Reject duplicate event IDs and mark late/stale status. Store event time and ingestion time separately; display the last-update time. Conflicting sources enter review rather than letting a model select the more convenient one.

03 / Prepare a factual message

Responsible: Template engine; optional AI editor

Include what changed, quantity/location, source timestamp, action requested, deadline and a safe first-party reference link. Start with deterministic templates. If AI translates or summarizes, retain the source, disclose estimates and require review for commercial/legal or sensitive messages.

04 / Route privately and track delivery

Responsible: Notification service + coordinator

Use authorized role recipients and agreed contact preferences. Do not include personal wage data, bank instructions or confidential prices in public notifications. A future provider queue uses idempotency, bounded retries and a failed-delivery queue. No email/SMS provider integration is currently asserted.

05 / Require an accountable response

Responsible: Recipient

Acknowledge receipt separately from accepting a new commercial term. Add a reason, evidence or proposed revised date. A revised price/date/quantity becomes a pending order amendment requiring the proper parties, never an automatic contract update.

06 / Escalate and close with evidence

Responsible: Coordinator + responsible party

Escalate unacknowledged or overdue actions to the named backup, then record resolution and supporting reference. The coordinator cannot close a disputed physical fact just because the message was delivered. Export the action history and measure recurring causes.

CONTROLS AND IMPLEMENTATION

Make exceptions visible

Failure handling and human safeguards

Wrong recipient or changed authority: revoke access and reroute. Failed channel: use the agreed manual/telephone fallback and record it. AI translation ambiguity: show the original and request human clarification. Stale logistics feed: label unknown and contact the source, rather than promising an arrival date. Urgent safety concerns follow the separate safeguarding/emergency route.

Blockchain, AI and private evidence

Add an outbox in the same database transaction as the business event so an accepted change cannot silently lose its notification task. A worker sends with retry/deduplication, records provider status and never treats a delivery callback as business approval. AI is optional; blockchain stores only an approved audit digest after activation, not message content or contact details.

Start with the existing pilot

Use existing order/fulfilment records and a coordinator-managed action register; send agreed messages manually from authorized business channels. Capture acknowledgements and failures in the register. There is no active platform SMS/email-notification worker or automated AI translator.

Additional software required

Add transactional outbox, event templates, role/contact preferences, retry/dead-letter handling, acknowledgements, due-time escalation and amendment records. Complete provider privacy/security review and country/channel rules before sending live automated messages.

Current boundary: invited profiles, lot/order records and approvals, selected fulfilment events, invoices, operator-attested receipts, balances and protected private audit are configured. Several actions are API-only. Public blockchain worker, payments/crypto/escrow, AI, bidding, public passport resolver, evidence-vault uploads and the richer registers described here are not activated by publishing this design. Roles are proposed functions to assign and resource, not additional named team appointments.

PILOT AND COMMERCIAL VALIDATION

Prove the mechanism before scaling

Synthetic worked scenario

Simulate a dispatch delay, one lost email, duplicate event ingestion, a receiver mismatch and a stale feed. Set an agreed test acknowledgement target, then measure actual latency and the fallback burden; do not advertise instant updates from manual sources.

Required acceptance tests

Deliver the same event twice; change a recipient's authorization; inject an invented ETA; fail the provider; try to amend a price via acknowledgement. Each must preserve one action record, appropriate access and explicit contract reapproval.

Measures and go/no-go

Event-to-notice latency with freshness disclosed; acknowledgement time; overdue actions; delivery failures resolved; messages causing a false commitment (target zero in scripted tests). Compare manual coordination time before and after.

Proposed payer, charging unit and cost drivers

Proposed payer: business subscription or scoped coordination service, with message overage capped and disclosed in USD. Cost drivers are provider messages, support and exception handling, not the mere number of blockchain transactions.

Pilot sign-off record

Before execution, assign the actual responsible people, permitted data source, cohort/route, approved costs, test dates, evidence reviewer and release authority. Record each test outcome, unresolved exception, manual fallback and rollback procedure. Do not activate an unapproved model, payment provider, public-chain transaction or unsafe equipment connection.

Source and scope

COTO presentation slides 137. Detailed operating steps, test cases and commercial units are new implementation proposals. Read operating-model.pdf for shared controls, templates, release gates and primary technical references. The legal pack remains draft until completed and reviewed.