COMMON OPERATING MODEL / 01

A common operating spine

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.

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.

Start from accountable parties

Invite the chosen businesses, record their actual role/authority and review the relevant evidence. Complete the correct operator, seller-buyer, producer and service agreements from the draft legal pack before relying on them. Name an operations owner, source/quality reviewer, finance reviewer, data/security owner and appeal/safeguarding contact; these are roles to staff, not assumed appointments.

One shared commercial record

Demand/quote -> approved design and lot -> separately approved order -> controlled production/custody -> receipt/inspection -> invoice/receipt reconciliation -> aftercare. Carry the same order, lot/item, document version and event references. Keep physical possession, legal title, acceptance and payment as separate records.

Manual first, then controlled integration

A reviewed spreadsheet/register can test source quality and decision rights before software is built. The current API can support selected trade steps; do not pretend it enforces the proposed multi-site, two-person or partial-line controls yet. No automated financial instruction is permitted by these documents.

Provenance, accountability and transparency

Provenance links each assertion to its source and physical item. Accountability assigns an actor, approver, time and reason. Transparency provides the right viewer with the relevant evidence status, fees, gaps and freshness, not unrestricted access to confidential prices or personal data.

COMMON OPERATING MODEL / 02

Data, blockchain and AI controls

Canonical event envelope

Use event_id, event_type, object/order/lot references, actor business and role, source system/external ID, event_time/timezone, received_time, location, quantity/unit where applicable, evidence reference/digest, review status, previous version and any correction reference. Validate required fields and units and preserve original source records. GS1 EPCIS provides a useful event-model reference; no GS1 compliance or certification is claimed.

Evidence and permissions

Keep documents and personal data off-chain. The current pilot supports descriptions and fingerprints, not a private document-upload service. A future vault needs least-privilege access, authorized retrieval, malware/size checks, retention/holds, correction and export. Avoid worker names/identity records in public item views; no individual employment/credit/eligibility scoring.

Controlled blockchain route

Reuse the existing canonical salted SHA-256 audit approach and registry sequence per opaque stream. Before activation, approve network/RPC, exact deployed contract, owner/writer custody, fee ceiling and confirmation rule. Journal the exact signed transaction before broadcast; reconcile receipt/block hash and stop on changed confirmation or unexplained state. Pending anchor is distinct from reviewed fact. No AMN-coin peg, 50 ms performance or automatic bank payment is claimed.

AI decision support

Govern: assign owners and data/vendor permissions. Map: define the limited decision and affected people. Measure: compare to a representative labelled/manual baseline. Manage: enforce budget, human approval, failure handling and rollback. Record model/version, input window, source, uncertainty and reviewer outcome. Use deterministic rules where adequate; a model must not silently change a contract, release funds, reject a warranty or certify labour conditions.

COMMON OPERATING MODEL / 03

A proposed 30-day pilot

Days 1-5: define and prepare

Suggested sequence, not a delivery commitment. Select a small voluntary cohort and one supply route, agree staff time, secure evidence exchange, privacy/local-language arrangements and relevant contracts. Establish current baseline times/costs. Freeze identifiers, quantities, locations and review/exception definitions. Use synthetic data until the checks and permissions are ready.

Days 6-12: run the records

Exercise lot/order approvals, stock reservation and synthetic invoice/receipt reconciliation. Run richer custody, design, producer-pay and exception registers manually. Reconcile totals daily. The proposed independent reviewer checks high-risk attestations; current application permissions alone do not enforce all planned segregation.

Days 13-20: exercise the eight mechanisms

Test QR identity, missing lineage, comparable quotes, design sample approval, notification failure, production-unit errors and aftercare/duplicate credits. AI remains shadow/manual unless an approved data route and model are available. No public-chain or real-money trial is implied.

Days 21-30: assess and decide

Review source completeness, staff burden, unresolved exceptions and baseline comparisons. Close every scripted financial/authorization/privacy failure or keep the affected feature disabled. Obtain operational and legal sign-off on actual service claims. Select at most one justified automation next; a successful synthetic pilot is not evidence of customer revenue or a production launch.

COMMON OPERATING MODEL / 04

Operating pack and release gates

Registers provided

Use the event register, RFQ/allocation register, physical passport/tag register, design/sample approval register, action/notification register, production/material register, case/remedy register and separate USD settlement register. Headers are templates, not API endpoints. Record preparer, checker, authority and source evidence; do not store live credentials or unnecessary personal data in shared spreadsheets.

Measure cost as well as speed

For each enabled service, measure staff minutes, independent review, assisted participation, hardware/vendor charges, support/rework and overhead allocation. Proposed fee units in the eight runbooks are not prices. A viable USD tariff must cover legitimate service costs under a signed scope; gross carpet trade value and client funds are not automatically COTO revenue.

Go / no-go

Do not progress a feature with unresolved cross-business data exposure, duplicate allocation/payment handling, unapproved model use, unsafe site control, invalid contract authority or harm to producer pay/complaint rights. A failed or unavailable provider is a visible state with a manual fallback, not an excuse to label a trade settled. Keep record exports and a restore/recovery drill in the release plan.

Accountable approval

Before a real feature release, record the actual operating/legal entity, named accountable owner, process/evidence reviewer, data/security sign-off, legal/payment-provider approval where needed, approved costs, test evidence, rollback method, customer disclosure and effective version. No new AWS resources, billable model service, wallet, provider account or transaction is created by this pack.

Primary references

GS1 EPCIS event guidance - official reference

NIST AI RMF core - official reference

ICC: Incoterms, title and sale terms - official reference