

USE CASE 02 / COTO PPT 55

Traceability and accountable evidence

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

Build a product history that can be checked against real sources, quantities and locations, with explicit confidence and missing-link labels.

Accountable roles

A data steward owns the event dictionary; producers and custodians attest their own events; an independent quality/source reviewer checks claims according to the agreed scope.

Required information

Unique item/lot IDs; parent-child material batches; event ID; event time plus time-zone offset and received time; actor/business/site reference; event type; quantity/unit; source document version/digest; claim scope and review status; correction/reversal references.

Separate lifecycle states

Event: captured > validated > attested > reviewed OR rejected > corrected/superseded. Handover: sender-attested > receiver-confirmed OR discrepancy. Anchor: pending > submitted > confirmed OR failed/recheck-required, tracked separately from evidence review.

THE OPERATING WORKFLOW

From a real input to an approved outcome

01 / Create one identity and vocabulary

Responsible: Data steward

Allocate an opaque item/lot ID and documented event types: received, transformed, packed, dispatched, received-at-site, inspected, split, merged and corrected. Record units and location definitions. A future EPCIS mapping is a standards-alignment proposal, not current GS1 certification.

02 / Capture at the actual source

Responsible: Producer/site custodian

Record what happened, when, where, why and by whom, with the evidence reference. Assisted/offline intake is permitted but must preserve the original event time and the coordinator who entered it. Do not backdate an upload as if it were real-time capture.

03 / Validate quantity and duplication

Responsible: Rules + data steward

Reject duplicate external event IDs, impossible units, unknown actors, negative balances and child-lot quantities exceeding their parent. Quarantine inconsistent events instead of silently correcting them. Document legitimate process yield/waste separately.

04 / Review the claim rather than just the file

Responsible: Qualified reviewer

Label supplier-declared, evidence-checked, independently inspected, expired or disputed claims. Check the issuer, site/product scope and validity of certificates where relied on. Assess labour evidence through a proportionate human process, never facial/age inference or hash-based certification.

05 / Reconcile the handover

Responsible: Sender + receiver

Match dispatch and receipt by item/lot, place and quantity. A sender cannot confirm the receiver on their behalf. Physical stock counts and source records resolve differences; a one-sided handover remains visibly incomplete.

06 / Present a permissioned timeline

Responsible: COTO operator

Show source, review scope and last-updated time beside each material assertion. Export only the viewer-permitted fields. Append a correction with reason and superseded event reference, preserving the original and any necessary legal hold.

CONTROLS AND IMPLEMENTATION

Make exceptions visible

Failure handling and human safeguards

Missing source: mark unknown and request evidence; do not fill it with a model guess. Broken handover: show the gap. Duplicate IDs: quarantine both suspect uses until resolved. Expired certificate: remove the current-valid badge, retain historical scope. Suspected coercion: protect the reporter and route to the sourcing/grievance process, not an automatic supplier conviction.

Blockchain, AI and private evidence

Store full evidence in a proposed private evidence vault with restricted signed retrieval and retention rules; the current pilot stores descriptions/fingerprints, not document uploads. The existing canonical salted SHA-256 audit approach can anchor opaque digests through the disabled relayer after activation approval. Optional OCR/AI flags inconsistencies for people; deterministic quantity checks remain authoritative.

Start with the existing pilot

Use lots, maker-group reference, origin/location, evidence description/digest and protected audit exports. Pilot richer event capture in the supplied event register with named attestations and manual document review through an agreed secure channel.

Additional software required

Add a structured event store with issuer permissions, idempotency, parent-child lineage, custody countersignatures, evidence-vault retention and event-level review status. Add import/export adapters only after testing the shared dictionary. A review-status field is not a certification service.

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

Trace one synthetic yarn lot into two carpet lots, then dispatch 12 pieces to warehouse A and eight to B. Reconcile all 20 with independent receipts; deliberately omit B's receipt and show the provenance gap until it is supplied.

Required acceptance tests

Try an over-sized split, duplicate import, changed evidence file and reversed handover; confirm the history remains visible, quantities conserve within the declared process and each viewer sees only permitted fields.

Measures and go/no-go

Percent of required events with source and accountable actor; physical-to-record differences; missing handovers; certificate expiry detection; correction resolution time. Pilot gate: detect every deliberately injected lineage and quantity exception.

Proposed payer, charging unit and cost drivers

Proposed payer: business subscriber or scoped supply-chain programme. Unit: supported lot/event volume and review service, with independent inspection quoted separately. Measure review effort, storage and connector maintenance; do not sell an unsubstantiated ethical badge.

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 55. 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.