IMS · WORKED-EXAMPLE AUDIT TRAIL

From signal to verified delivery

One synthetic incident · followed through the seven IMS pipeline phases

PURPOSE
Procurement-grade walkthrough of how IMS handles one incident end-to-end.

AUDIENCE
Procurement officers · security/audit teams · institutional ICT reviewers

DATA
Synthetic — illustrative of a real-world Darfur corridor incident pattern

METHODOLOGY VERSION
v1 (in production since 2026-04) · /ims/methodology

WORKED-EXAMPLE HASH
bd6f90e1…cd02

This document does NOT represent a real operational brief.
It is a worked walkthrough that an evaluator can compare against
the system's behaviour in a live pilot.

Each subsequent page represents one phase of the IMS pipeline.
Every claim made on every page is backed by code in production
today — see /ims/methodology for the engineering description.

PHASE 1 OF 7

Signal arrival

4 raw records ingested · clock spread: 10 minutes

Each ingestion record carries source slug, original URL, original publish timestamp, raw payload, and our ingest timestamp. The raw payload is preserved for audit and never shown unless an admin opens the audit log.

Raw records (this incident):

01	ReliefWeb Convoy attacked on El Fasher–Tawila road, North Darfur *https://reliefweb.int/report/sudan/situation-report-042-2026*	2026-04-23 12:04:00 UTC
02	AFP Sudan: armed group attacks aid convoy near El Fasher *https://wires.afp.com/2026/04/23/sudan-convoy-attack*	2026-04-23 12:07:00 UTC
03	OCHA Sudan Flash update: humanitarian convoy targeted, North Darfur *https://reports.unocha.org/sudan/flash-2026-04-23-darfur*	2026-04-23 12:09:00 UTC
04	Local channel (verified) Reports of attack on aid corridor — Tawila road *telegram:verified-channel-id-4471*	2026-04-23 12:14:00 UTC

PHASE 2 OF 7

Deduplication & clustering

4 records → 1 incident (entity overlap + geo proximity + temporal window)

Clustering decision uses three independent signals — never text similarity alone. For this synthetic incident:

- Entity overlap : {El Fasher, North Darfur, convoy} present in 4/4
- Geographic proximity : all coordinates within 8 km radius
- Temporal window : all 4 within 6-hour breaking-event window

Decision: cluster as one incident. Promote canonical record id
incident_id = 5f82-4471
Subordinate records are linked to the canonical for audit but no longer surface as separate cards.

PHASE 3 OF 7

Cross-corroboration

≥ 2 sources of distinct type required for VERIFIED status

Source-type taxonomy applied (single-type clusters are flagged but never promoted to VERIFIED, never shown on the public marketing preview).

Sources contributing to this incident, by type:

- humanitarian-sitrep (ReliefWeb)
- newswire (AFP)
- humanitarian-sitrep (OCHA Sudan) [same type as ReliefWeb — does not count]
- curated-local-channel (verified Telegram)

Distinct types present: 3 (humanitarian-sitrep, newswire, curated-local-channel).
Threshold for VERIFIED: 2.
Decision: PROMOTE TO VERIFIED.

PHASE 4 OF 7

Brief generation

Analyst clicks 'Generate brief' · brief_id = 4f8a-e21c

The brief is composed deterministically from the canonical incident and any additional incidents the analyst dragged into the side panel. Section structure is templated; section CONTENT is fact-stitched from the underlying records (no free-form LLM-generated analyst text).

PDF artefact emitted with:

- Classification banner (default: OFFICIAL USE ONLY · IMS BRIEF)
- Reporting period, generation timestamp, generating user
- Per-incident source citations with timestamps
- SHA-256 hash over the canonical content payload

For this worked example, the synthetic brief hash is bd6f90e1…cd02 (also shown in this document's own footer).

PHASE 5 OF 7

Forward to superior

Analyst sends brief via secure link · audit-log row written

BRIEF ID
4f8a-e21c

FROM
desk-officer · East Africa · authenticated session sess-19a4

TO
Regional Security Adviser · East Africa

CC
Country Director · Sudan

SUBJECT
North Darfur Corridor — situation brief 22-25 Apr

SECURE LINK
https://ims.app/b/4f8a-e21c · expires 7d · download tracked

AUDIT ROW
forward-event id evt-7c12 · ts 12:19:00 UTC

PHASE 6 OF 7

Recipient opens & verifies

Each open writes an audit row · SHA-256 verifiable offline

Subsequent opens of the brief append further audit rows. The full audit log is queryable by any user with read-access to the brief.

- 2026-04-23 12:23:00 UTC
  Opened from Nairobi · IP-checked · session sess-9f3b
- 2026-04-23 12:27:00 UTC
  Forwarded to Country Director, Sudan (auto-cc fired)
- 2026-04-23 12:33:00 UTC
  PDF downloaded · SHA-256 verified by client offline
- 2026-04-23 12:35:00 UTC
  Brief acknowledged with reply note: 'received, briefed director'

PHASE 7 OF 7

Tamper detection in the field

What happens if someone modifies the PDF after delivery

The SHA-256 hash in the footer is computed over the canonical content payload (rows + metadata, JSON-canonical, sorted keys). The algorithm is published — independent verification needs no proprietary tool.

Verification steps any reader can perform offline:

1. Note the hash from the footer.
2. Request the canonical payload via the API (or from sender).
3. Run sha256sum locally on the canonical payload.
4. Compare.

If the hash matches → the brief is exactly as generated.
If the hash does not match → the file has been altered, OR the canonical payload provided is wrong. Either way, the discrepancy is visible and worth investigating.

We do not require trust in IMS for verification. We require trust in SHA-256, which is widely-trusted and independently implementable.

CLOSING

What this artefact is for

How to use this PDF in your evaluation

Hand this document to the security / audit / procurement team that will evaluate IMS. It demonstrates the workflow at the depth they need, without requiring access to a live pilot.

Then, in your pilot, run a single real incident through the same seven phases and compare the trail to this document. The system should behave exactly as described here — same audit-row structure, same hash discipline, same source-citation format.

If anything diverges, that is a bug we want to know about:
trust@quintarthai.com

Methodology: https://ims.quintarthai.com/methodology.html
Source registry: https://ims.quintarthai.com/sources.html
What we don't have yet: https://ims.quintarthai.com/gaps.html
Founding cohort: https://ims.quintarthai.com/founding.html