**Story — “Sanctions Feed → Trust-Stamped Snapshot → Safe Activation”**

**Intent (one line)**

Keep screening **always correct and defensible** by turning each provider release into a **trust-stamped snapshot** that can be **simulated, proven, and safely activated**—without ever risking a silent ALLOW.

**Business Outcome**

* Zero “we didn’t know” excuses. Every decision is linked to a **provable snapshot** + **explainable delta**.
* Ops can **simulate impact** before activation, avoiding accidental business disruption.
* Auditors get a one-click **Proof Bundle**: what was fetched, when, from whom, and why it changed outcomes.

**Actors**

* **Provider Feed Daemon** (pulls provider datasets)
* **Snapshot Foundry** (makes immutable snapshots + stamps trust)
* **Delta Lab** (computes & visualizes changes; runs impact simulation)
* **Ops Pilot** (human who promotes/rolls back with guardrails)
* **Screening Engine** (uses the currently active snapshot)
* **Audit Vault** (stores proofs, receipts, decisions)

**Preconditions**

* Provider API keys configured.
* Dataset Registry exists (dataset → policy bucket: *HARD\_BLOCK*, *HOLD*, *REVIEW*, *ADVISORY*).
* KMS signing keys live (for trust stamps).
* Tenant policies loaded (authority precedence, bucket behavior).

**End-to-End Flow (happy path)**

**1) Fetch (Provider-First)**

* Provider Feed Daemon detects a **new release** (webhook or schedule).
* It retrieves the raw payload(s) and saves verbatim artifacts to **Cold Room** storage with exact headers + retrieval timestamp.

**2) Mint a Trust-Stamped Snapshot (Snapshot Foundry)**

* Normalize **without loss** (keep originals side-by-side).
* Compute **content hash** on provider-canonical form.
* Produce a **Trust Stamp**: {snapshot\_id, provider, dataset\_id, release\_id, retrieved\_at, content\_sha256, signer\_key\_id, signed\_at}.
* Store it immutably in **Snapshot Vault**.

Innovation 1 — **Trust Stamp as a “Receipt”**: A short, signed receipt you can hand to auditors or even embed as a QR in reports.

**3) Delta Lab (Context Before Consequence)**

* Compare with last ACTIVE snapshot for that dataset.
* Build an **Explainable Delta**:
  + **Impact Heatmap** (added / removed / changed entities by authority, country, program).
  + **Risk Tilt Score** (does this release skew higher risk vs last release?)
* **No activation yet.**

Innovation 2 — **Impact Simulator**: Before making it live, Delta Lab replays the new snapshot against **recent partners + open transactions** to show **who would flip to REVIEW/BLOCK**.

**4) Safety Gate (Human-in-the-Loop, Smart Defaults)**

* If delta is “normal”: auto-eligibility for **Progressive Activation** (below).
* If delta is “spiky” (e.g., >X% removals, schema drift), system goes to **“Hold for Pilot Review”** and recommends a **Shadow Match** run first.

Innovation 3 — **Progressive Activation**:

* **Phase A (Shadow)**: Engine matches with **new snapshot in parallel**, but gates still obey **current** snapshot; Ops sees differences live.
* **Phase B (10% Tenants)**: Activate for lowest-risk tenants; watch metrics.
* **Phase C (Global)**: Activate broadly once guardrails pass.

**5) Activate Snapshot (No Partial State)**

* Matching Index swaps atomically to the **ACTIVE** snapshot (no half-loaded lists).
* Publish **ListSnapshotActivated** event (tenant-aware).
* Screening Engine immediately references the new snapshot\_id.

**6) Rescreen & Gate Refresh (Only What Matters)**

* Queue **Impacted Entities** (from simulator + delta keys):
  + Partners with name/identifier overlaps.
  + **Open orders/deliveries/invoices** connected to those partners.
* Recompute decisions → **push only deltas** to connected systems.
* Gates flip accordingly (ALLOW → HOLD/DENY) **within tenant SLAs**.

**7) Audit Bundle (Tamper-Evident, Shareable)**

* For each activation, create a **Proof Bundle** (downloadable):
  + Trust Stamp, raw provider headers, counts, Delta Heatmap, Simulator summary, who approved activation, when, and why.
* Every screening decision stores snapshot\_id + **Trust Stamp hash** for later verification.

**Alternate / Failure Flows**

**A) Schema Drift Firewall**

* If provider schema changes, **Foundry pauses**; marks dataset “Needs Mapping.”
* Delta Lab shows **Field Drift Map** with suggested mappings.
* No activation allowed until Ops accepts mapping.
* Screening continues on last ACTIVE snapshot; **high-risk buckets default to REVIEW**, never silent ALLOW.

Innovation 4 — **Drift Firewall**: A hard barrier that prevents bad schema pushes from changing production behavior.

**B) Suspicious Delta Quarantine**

* Massive adds/removes or authority contradictions → **Quarantine Mode**.
* Run **Shadow Match** only; require **Dual Attestation** (two Ops users) to promote.

Innovation 5 — **Dual Attestation with Reason Codes** logged into the Proof Bundle.

**C) Provider Stale / Outage**

* Keep last ACTIVE snapshot.
* **Staleness Banner** visible in consoles + tenant-visible (“Using provider data from HH:MMZ”).
* **Risk-Weighted Fallback**: for buckets marked **HARD\_BLOCK**, new activity defaults to **REVIEW**; for non-critical advisory buckets, continue ALLOW.

**Acceptance Criteria**

1. **Trust-Stamped Snapshots**
   * Every dataset release results in a **signed snapshot** with a unique snapshot\_id and reproducible content\_sha256.
2. **No Partial Activations**
   * Index swaps are atomic; Screening Engine always uses a single, coherent snapshot.
3. **Explainable Deltas**
   * Delta Lab renders a **Heatmap** + **Risk Tilt Score** and lists **impacted partners/transactions** prior to activation.
4. **Progressive Activation Works**
   * Shadow → 10% → Global sequence is available; Ops can roll back instantly with a click; rollbacks restore prior snapshot and emit an event.
5. **Fail-Safe Defaults**
   * Schema drift, suspicious delta, or provider stale **never** causes silent ALLOW for high-risk buckets; the system defaults to **REVIEW**.
6. **Audit Proof Bundle**
   * For any activation, an auditor can download a bundle containing Trust Stamp, deltas, simulator results, approvals, timestamps—**and reproduce** any past decision bit-for-bit.

**Non-Functional Targets**

* **Activation latency:** ≤ **5 min** from provider release retrieval to ready-to-activate snapshot.
* **Rescreen completion:** ≥ **95%** of impacted items processed within tenant SLA window.
* **Availability:** 99.9% ingestion pipeline success / month.
* **Cost discipline:** Storage tiering (hot 90d, warm 1y, archive 7–10y); simulator runs are scoped to **impacted** entities only.

**AI (Assistive, never the decider)**

* **Delta Narrator:** LLM writes a clear human summary of what changed (checked against facts from the delta).
* **Drift Mapper:** Suggests new field mappings when schema shifts (Ops accepts/edits).
* **Impact Forecaster:** Predicts which tenants will see the biggest operational effect; proposes **staggered activation** order.
* **Evidence Composer:** Builds the Audit Proof Bundle narrative for Ops to approve.

*All AI outputs are* ***cited****,* ***overrideable****, and logged; decisions still come from rules + provider data.*

**Original Innovation Checklist (your “moat”)**

* **Trust Stamp Receipts** (QR-ready, KMS-signed)
* **Impact Simulator** + **Risk Tilt Score** before activation
* **Progressive Activation** (Shadow → 10% → Global) for data releases
* **Drift Firewall** + **Dual Attestation** on risky changes
* **Explainable Delta Heatmaps** per authority/program/country
* **One-click Audit Proof Bundle** tied to every decision