**6) Access Reviews & Segregation of Duties (SoD) — “Trust, Re-attested”**

**Intent**  
Ensure only the right people can do the right things — and that overrides are rare, justified, and double-checked.

**Actors**  
Access Review Engine • SoD Policy Engine • Approvers • Auditors • KMS Notary

**Preconditions**

* Roles defined (Viewer, Operator, Reviewer, Approver, Admin).
* Critical actions flagged (override release, rules activation, license counter edit, merge partners).

**Flow**

1. **SoD Policies**: e.g., “No one can both create a license **and** approve a blocked shipment using it.”
2. **JIT Elevation**: temporary role boost via ticket + MFA; expires auto.
3. **Override Notarization**: any override creates a **Notarized Entry** (payload hash + reason + approver + timestamp, KMS-signed).
4. **Quarterly Campaigns**: managers re-attest their team’s access; non-responses auto-revoke.
5. **Toxic Combo Detector**: real-time block when a user’s roles violate SoD; suggests alternate approver.
6. **Review Dashboard**: shows overrides by user, reason taxonomy, anomaly spikes; one-click revoke.

**Acceptance**

* 100% critical overrides have a Notarized Entry with reason + approver.
* Quarterly attestation completion ≥ 98%; dangling accounts auto-revoked.
* Attempts to perform toxic combinations are **blocked** with auditable message.

**Innovations**

* **Notarized Overrides** (KMS-signed facts).
* **Toxic Combo Detector** with live guidance.
* **JIT Elevation** that decays automatically.