**Track A — Front-end (dashboard) *(summary only for now)***

* Live Ops (triage queues, KPIs, bulk actions), License Hub (counters/expiry), Rules Lab (low-code builder + simulation), Master Data, Documents/OCR, Audit Vault, Settings/Integrations with SSO/RBAC/ABAC. These surfaces sit on top of the API you’ll build below.

ComprehensiveRequirementsforaBe…

**Track B — Back-end (API + engines) — what to build now**

**0) Sprint-0 exit criteria (what “ready” looks like)**

* **OpenAPI v1** published (HTML/JSON) with mock servers passing contract tests.
* **SLOs** agreed; error budgets/alerts in place; Dev/Stage environments via IaC; blue-green/canary demo.
* **SSO/MFA** wired; role matrix and **ABAC** policies enforced on mock endpoints.
* **Residency/retention** policies codified; DR restore test executed.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**1) API v1 surface (define & stub today)**

**Principles**: /api/v1, OAuth2 client-credentials + OIDC, Idempotency-Key on POSTs, 600 rpm/tenant default, consistent error schema with trace\_id.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**Core endpoints to implement first**

* POST /determine → returns **ALLOW/REVIEW/BLOCK + WHY/FIX + audit\_id**
* POST /simulate → what-if using draft rules, no side effects
* GET/POST /rules and /rules/{id}/deploy → CRUD + lifecycle
* GET/POST /masterdata/products and /masterdata/parties
* GET /sanctions/sources, POST /sanctions/refresh
* POST /documents (upload), GET /documents/{id} (versions/metadata)
* POST /webhooks/subscriptions (+ outbound: determination.created, status.changed)
* POST /integrations/sap/so (sales-order upsert adapter)

LicenseIQ\_BoardReady\_Requiremen…

**Standard error** (all endpoints):  
{"error":{"code":"string","message":"string","details":[{"field":"","issue":""}],"trace\_id":"uuid"}}

LicenseIQ\_BoardReady\_Requiremen…

**2) Core domain services (MVP scope)**

**a) Rules/Determination Service**

* Evaluate per line: product→ECCN/HS, destination, parties, content % (de-minimis), quotas.
* Determination pipeline: **Trigger → Apply rules → De-minimis → Quotas → Decision (license/exception) → WHY/FIX**.
* Data model: Rule(id, condition, action, priority), LicenseType, Quota.

ComprehensiveRequirementsforaBe…

ComprehensiveRequirementsforaBe…

**b) Rules Lifecycle/Governance**

* Draft → **shadow test** (mirrored traffic, read-only) → **canary** (≤10%) → prod; one-click rollback; 4-eyes approval.
* Before risky changes: simulation on last 90 days.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**c) Master Data Service**

* **Products/Materials**: HS, ECCN, dual-use flag, origin, BOM %, licensing notes.
* **Parties/Customers**: identifiers (DUNS/LEI), addresses, type, SPL screening status, risk score, KYC refs.
* CRUD + bulk import (ERP/CSV/API); dedupe; mapping ECCN↔HS; scheduled refreshes.

LicenseIQ\_BoardReady\_Requiremen…

ComprehensiveRequirementsforaBe…

**d) Sanctions Sync Service**

* Sources: OFAC, EU, UN (+ local regimes). Persist **source timestamps & deltas**; expose freshness via /sanctions/sources.

LicenseIQ\_BoardReady\_Requiremen…

**e) Documents/OCR Service**

* Upload → async OCR → metadata extraction → link to orders/licenses; versioning; retention 5–7y.
* Entities: Document, TransactionLink, Metadata. Webhook on OCR complete.

ComprehensiveRequirementsforaBe…

ComprehensiveRequirementsforaBe…

**f) Audit & Evidence Service**

* Immutable event log for auth, permission changes, rule deploys, determinations, exports.
* Every /determine returns **WHY/FIX** with rule IDs + cited sources; downloadable evidence pack.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**g) Integrations Gateway**

* SAP SO adapter (POST /integrations/sap/so); ERP/CRM sync jobs (JSON/XML/CSV + EDI 810/856 baseline); outbound webhooks.

LicenseIQ\_BoardReady\_Requiremen…

ComprehensiveRequirementsforaBe…

**3) Non-functional baselines (build in from day 1)**

* **Performance**: rule eval **p95 ≤ 500 ms** (≤50 lines); OCR **p95 ≤ 5 s** first-page <2 s.
* **Availability**: target **99.95%** Y1; **DR** RPO ≤ 1 h / RTO ≤ 4 h.
* **Scale**: baseline 50 TPS; load-test to 200 TPS.

LicenseIQ\_BoardReady\_Requiremen…

Expert Review of the Comprehens…

**Security & privacy**

* SSO (OIDC/SAML), **MFA**, **RBAC + ABAC** (region, BU, customer-group); per-tenant keys & rate limits.
* TLS 1.3, AES-256-GCM at rest; secrets in KMS/Vault with 90-day rotation.
* Residency pinning (EU→EU, US→US); retention: ops 7y, logs 13m; DSR/DPIA processes.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**Observability & reliability**

* Structured JSON logs, metrics (latency, error\_rate, saturation), distributed tracing; burn-rate alerts; on-call runbooks.

LicenseIQ\_BoardReady\_Requiremen…

**4) Data model (initial schemas)**

**Products/Materials**: material\_id, sku, description, uom, category, hs\_code, eccn, dual\_use\_flag, origin\_country, bom\_pct, licensing\_notes, controlled\_reasons  
**Parties/Customers**: party\_id, external\_ids{duns, lei}, tax\_ids, name, addresses, country, region, party\_type, screening\_status, risk\_score, last\_reviewed\_at, kyc\_docs  
These are the minimum fields the engine and UI filters depend on.

LicenseIQ\_BoardReady\_Requiremen…

**Rules/Quotas**: Rule(id, condition, action, priority), LicenseType(id, code, jurisdiction, validity\_period), Quota(id, license\_id, remaining\_qty, reset\_date)

ComprehensiveRequirementsforaBe…

**Documents**: Document(id, type, version, status, upload\_date, expiry\_date), TransactionLink(document\_id, order\_id, license\_id), Metadata(document\_id, tag\_key, tag\_value)

ComprehensiveRequirementsforaBe…

**5) Services breakdown & sequencing**

**Phase 1 — “Core decision loop”**

1. **Determine API** (sync) + **Audit** write.
2. **Master Data** minimal CRUD (products/parties).
3. **Sanctions** source table + freshness endpoint.
4. **Rules** evaluator with a handful of high-value rules (ECCN×destination, party SPL hit, de-minimis, quota>80% alert).

ComprehensiveRequirementsforaBe…

**Deliverables**: OpenAPI for above endpoints; unit tests for rules; golden test fixtures (sample orders); p95 latency dashboard.

**Phase 2 — “Rules Lab + Simulation”**

* Draft/Deploy states, **shadow** & **canary** paths; POST /simulate using last-90-days dataset; one-click rollback.

LicenseIQ\_BoardReady\_Requiremen…

**Phase 3 — “Licenses & Quotas”**

* License models, counters, reserve/release API; 80%/90% depletion alerts.

ComprehensiveRequirementsforaBe…

**Phase 4 — “Docs & OCR”**

* Async OCR pipeline + versioning; link docs→orders/licenses; retention jobs.

ComprehensiveRequirementsforaBe…

**Phase 5 — “Governance & Evidence”**

* Evidence pack generator (compiles WHY/FIX, rule IDs, sources, doc links) and admin audit timelines.

LicenseIQ\_BoardReady\_Requiremen…

**6) DevOps & platform (set up now)**

* **CI/CD**: trunk-based; PR checks (unit/integration/load tests, lint, **SAST/DAST**, license scan); signed images; SBOM published.
* **IaC**: Terraform + Helm; envs: Dev/Stage/Prod.
* **Deployments**: blue-green/canary with SLO gates & automated rollback.
* **Monitoring**: metrics/logs/traces dashboards per service; burn-rate alerting.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**Suggested stack** (per expert review):

* **Backend**: Python or Java for rules; Node.js for real-time adapters.
* **Data**: PostgreSQL (relational), object store for docs, Redis for caches (quotas, sanctions).
* **Containers/Orch**: Docker + Kubernetes (cloud/on-prem).

Expert Review of the Comprehens…

**7) Security hardening (baseline)**

* Central **secrets vault**, 90-day rotation; **TLS 1.3**; **AES-256-GCM** at rest; per-tenant rate-limit + keys.
* Log auth events, permission changes, rule deployments, exports to SIEM; anomaly alerts.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**8) Test strategy**

* **Contract tests** for API v1 (mocked services must pass in CI).
* **Unit tests** for rules (truth tables), **simulation** diff tests, **load tests** to verify p95 targets.
* **DR drill** (restore from backup) and **residency** checks (EU data pinned to EU).

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…

**9) “Definition of Done” for Back-end MVP**

* Endpoints from §1 online with **idempotency**, **rate limits**, and **WHY/FIX** in responses.
* Rule lifecycle (draft→shadow→canary→prod) enforced with 4-eyes approval & rollback.
* Master data CRUD with explicit fields; sanctions freshness visible; audit evidence export available.
* Observability dashboards & SLO alerts live; CI/CD deploys to Dev/Stage via IaC.

LicenseIQ\_BoardReady\_Requiremen…

LicenseIQ\_BoardReady\_Requiremen…