LicenseIQ — Board■Ready Requirements Addendum v1.0

Date: Sep 16, 2025

LicenseIQ — Board■Ready Requirements Addendum v1.0

Date: Sep 16, 2025
This addendum patches gaps in the existing functional requirements by specifying **non■functional baselines**, **security & privacy controls**, **DevOps/observability**, **API v1 contract outline**, **i18n**, **extensibility**, **change governance**, **training/docs**, and **explicit master data fields** for Customers and Materials. It is designed to be approved by the Board and used by Engineering as Sprint 0 acceptance criteria.

1) Executive Summary of Additions

• **NFR/SLOs**: Clear performance, availability, scalability, DR, and accessibility targets.
• **Security & Privacy**: OIDC/SAML SSO, MFA, RBAC/ABAC, encryption, data map, residency and retention with DPIA.
• **API v1**: Versioned REST with authentication, idempotency, rate limits, error schema, pagination, and webhooks.
• **DevOps & Reliability**: CI/CD, IaC, blue■green/canary, metrics/logs/traces, error budgets, on■call runbooks.
• **Change Governance**: Draft → shadow test → canary → production with 4■eyes approval and rollback plan.
• **i18n & Accessibility**: Locale formats, currency, RTL, WCAG 2.2 AA.
• **Extensibility**: Plugin SDK for rules and reports with sandboxing.
• **Training & Docs**: End■user/Admin/Developer guides, API reference, and support SLAs.
• **Master Data**: Explicit fields for **Customers** and **Materials/Products** including HS/ECCN mappings.

2) Non■Functional Requirements (NFRs) & Service Level Objectives (SLOs)

Performance
• Rule evaluation: **p95 ≤ 500 ms**, **p99 ≤ 900 ms** for typical orders (≤ 50 lines).
• OCR parse: **p95 ≤ 5 s** per doc (first page < 2 s), async pipeline with status callbacks.
• Search/autocomplete: **p95 ≤ 300 ms** (cached), **p95 ≤ 700 ms** (cold).
• Dashboard initial load: **LCP ≤ 2.5 s** on 3G Fast; **INP ≤ 200 ms** (desktop).
Availability & Reliability
• Target **99.95%** (Year 1) moving to **99.99%** (Year 2).
• **DR**: RPO ≤ **1 hour**; RTO ≤ **4 hours**; quarterly restore tests.
• **MTTR** ≤ **30 minutes** for Sev■1 (automated rollback).
Scalability & Capacity
• Baseline: **50 TPS** eval; scale■test to **200 TPS** with linear degradation.
• Data growth: 10M documents, 5M master data rows; retention (see §4).
Compliance & Accessibility
• **WCAG 2.2 AA** for UI; **Section 508**-aligned.
• Browser support: last 2 versions Chrome/Edge/Firefox; Safari ≥ 16.

3) Security Architecture

Identity & Access
• SSO via **OIDC** (Okta/Azure AD/SAML bridge). **MFA** required for Admin/Approver.
• Roles: **Admin**, **Compliance Manager**, **Operator**, **Auditor**, **Integration**.
• **ABAC**: region = {"EU","US","APAC"}, business_unit, customer group; field■level redaction.
Secrets & Keys
• Central vault (e.g., AWS KMS + Secrets Manager / HashiCorp Vault). Key rotation every 90 days.
Encryption
• In transit: **TLS 1.3** only. At rest: **AES■256■GCM** (DB, object store, backups).
Logging & Monitoring
• Auth events, permission changes, rule deployments, and data exports logged immutably.
• Forward security logs to SIEM; anomaly alerts (impossible travel, brute force).
Tenant Isolation
• Strong logical isolation per tenant; per■tenant encryption keys; rate■limit per tenant.
Secure SDLC
• SAST/DAST, dependency scanning, container image signing, SBOM (CycloneDX).

4) Privacy & Data Residency

Data Map & Lawful Basis
• PII categories: names, email/phone, addresses, identifiers (DUNS/LEI), order refs.
• Lawful bases: contract, legitimate interest, consent where required.
Residency & Pinning
• EU tenants: data stored/processed in **EU region**; US in **US region**. Cross■border transfers via SCCs.
Retention & Minimization
• Operational data: 7 years (configurable per tenant). Logs: 13 months by default.
• Pseudonymize analytics; mask sensitive exports; DLP checks on downloads.
DSR & DPIA
• Data Subject Requests within 30 days; DPIA performed before go■live; incident response ≤ 72h notification.

5) API v1 Contract Outline

Principles
• Versioned base path: `/api/v1`; OAuth2 client■cred + OIDC; **idempotency■key** header for POST.
• Rate limits: default **600 rpm** per tenant (burstable). Pagination: `limit/offset` (max 1000).
Core Endpoints
• `POST /determine` → evaluates order lines; returns **ALLOW/REVIEW/BLOCK** + **WHY/FIX** + `audit_id`.
• `POST /simulate` → what■if with draft rules on historic orders (no side effects).
• `GET/POST /rules` (+ `/rules//deploy`) → rule CRUD + deployment workflow.
• `GET/POST /masterdata/products` (HS/ECCN, dual■use flags, BOM %) and `/masterdata/parties` (SPL flags).
• `GET /sanctions/sources` and `POST /sanctions/refresh` (OFAC/EU/UN sync).
• `POST /documents` (upload) and `GET /documents/` (metadata, versions).
• `POST /webhooks/subscriptions` and outbound webhooks `determination.created`, `status.changed`.
• `POST /integrations/sap/so` (adapter stub) for sales order create/update.
Standard Error Schema
{

"error": {
"code": "string", "message": "string", "details": [{"field":"", "issue":""}], "trace_id":"uuid"
}
}

6) DevOps, Reliability, & Observability

• **CI/CD**: trunk■based; PR checks (tests, lint, SAST/DAST, license scan); signed images; SBOM published.
• **IaC**: Terraform + K8s manifests/Helm; environments: **Dev/Stage/Prod**.
• **Deployments**: blue■green/canary with automated rollback on SLO breach.
• **Observability**: structured logs (JSON), metrics (latency, error_rate, saturation), distributed tracing; dashboards per service.
• **SLO/Error Budgets**: alert on burn rates (e.g., 2%/1h, 5%/6h). On■call rota and runbooks defined.

7) Change Management & Configuration Governance

• **Lifecycle**: draft → **shadow test** (read■only, mirrored traffic) → **canary** (≤10%) → **production**.
• **Approvals**: 4■eyes for rule and master■data changes; change tickets auto■generated from UI.
• **Rollback**: versioned rules; one■click revert; audit trail captures who/when/why.
• **Impact Analysis**: simulation on last 90 days of orders before enabling a breaking rule.

8) Internationalization & Accessibility

• Locales: en■US, en■GB, de■DE, fr■FR, es■ES, pt■BR, it■IT, ja■JP; extendable.
• Currency/date/number formatting via ICU; **RTL■ready** layout; translation keys externalized.
• **WCAG 2.2 AA**: color contrast, keyboard nav, focus states, aria■labels.

9) Extensibility (Plugin/SDK)

• **Rule Plugins**: deterministic, side■effect■free functions with schema■validated inputs/outputs; sandboxed with resource/time quotas.
• **Report Plugins**: data■access via read■only APIs; export to CSV/JSON.
• **Versioning & Compatibility**: semantic version pins; deprecation policy; tenant■level enable/disable.

10) Training, Documentation & Support

• **Docs**: User Guide, Admin Guide, Developer/API Portal (OpenAPI + examples), Release Notes/Changelog.
• **Training**: onboarding videos, interactive tours, sample data workspace.
• **Support SLAs**: Sev■1: 1h response/4h workaround; Sev■2: 4h/1d; Status page + incident comms templates.

11) Master Data — Explicit Fields

Customer/Party (minimum)
• identifiers: `party_id`, `external_ids` (DUNS/LEI), `tax_ids`
• names & addresses (structured), `country`, `region`
• `party_type` (end■user, reseller, carrier, broker), `screening_status` (SPL hit, cleared, pending)
• risk: `risk_score`, `last_reviewed_at`, `kyc_docs` refs
Material/Product (minimum)
• `material_id`, `sku`, `description`, `uom`, `category`
• **HS code** (import), **ECCN** (export), `dual_use_flag`, `origin_country`
• composition/BOM % (for **de minimis**), `licensing_notes`, `controlled_reasons`

12) Compliance Mapping (examples)

• **Sanctions**: OFAC SDN/NS■PLC; EU consolidated; UN; local regimes. Store **source timestamps** and deltas.
• **Export Controls**: US EAR (ECCN), EU Dual■Use, India SCOMET; map rules to reasons for control.
• **Auditability**: every determination returns **WHY/FIX** + citations of rule IDs & sources.

13) Sign■off Acceptance Criteria (Sprint 0 Exit)

• SLO doc approved; dashboards show SLO metrics; error budgets configured.
• SSO/MFA live in Dev; role matrix + ABAC policy enforced on mock endpoints.
• OpenAPI v1 published (HTML/JSON); mocked services pass contract tests.
• CI/CD green; IaC creates Dev/Stage; blue■green demo successful.
• Data map + residency policy approved; retention jobs scheduled.
• i18n scaffolding in UI; string keys externalized; RTL smoke test passed.
• Risk register + DR runbook approved; restore test executed successfully.

14) Risks & Mitigations

• **Integration churn** → Freeze API v1 and enforce with contract tests.
• **Performance regressions** → Load tests in CI; SLO■based deployment gates.
• **Compliance gaps** → DPIA before go■live; change advisory on new jurisdictions.
• **Operational toil** → Automate data imports/exports and alert triage; clear runbooks.

Appendix A — RACI (excerpt)

• **API Contract**: R(Architect), A(Product), C(Backend Lead), I(Frontend, QA)
• **Security Baseline**: R(Sec Eng), A(CTO), C(DevOps), I(Product, Audit)
• **Residency Policy**: R(DPO), A(General Counsel), C(Infra Lead), I(Product)

Appendix B — Sample Idempotency/Errors

• Header: `Idempotency-Key: `; server stores request hash and response for 24h.
• Errors conform to §5; include `trace_id` for correlation across logs/traces.