COMPLIANCE READINESS

Certification & Compliance Readiness Matrix

Design vs. operated status by control family. A diligence reference, not a certification claim.

Confidential · Self-assessment · Not legal advice

ISO/IEC 17025
Lab testing support

STRONG

Software is accreditation-supporting today.

ISO/IEC 27001
Information security

DESIGN-READY

Mapped; not yet operated/evidenced.

SOC 2 Type II
Trust services

DESIGN-READY

Needs production controls + audit window.

GDPR / CCPA
Data protection

STRONG DESIGN

Activates once auth + encryption land.

CONTROL-FAMILY READINESS

CONTROL FAMILY	DESIGNED	OPERATED	PRIMARY GAP / NOTE
Access control / authorization	✔	■	Permission service enforced in services; weak until identity is authenticated.
Authentication (edge / OIDC)	✔	✘	Actor from X-Actor-Id header (spoofable); OIDC not wired. Top blocker.
Encryption (at rest / in transit)	✔	✘	In-memory/JSON store; no durable DB or encryption at rest yet.
Audit & accountability	✔	■	Append-only audit in place; value redaction/hashing not implemented.
Change management / versioning	✔	■	Versioned rules & panels, shadow runs; CI/IaC controls not stood up.
Consent & data-subject rights	✔	■	Consent gating + data-rights workflows coded; needs auth + DPA templates.
Data residency / sovereignty	✔	✘	Deployment/infra concern; no production region deployment yet.
Records retention / de-identification	✔	✘	Policy modeled; not configured or enforced; no storage lifecycle.
Operations security (obs/backups)	✔	✘	No monitoring, alerting, backups, or restore testing yet.
Incident response / breach notif.	✔	✘	Runbook defined in docs; not operated or tested.
Supplier / vendor / DPA management	✔	✘	Integration registry exists; vendor inventory & DPAs not in place.
Input validation / ingestion safety	✔	■	Shared validation model + admin queues; file AV & real adapters pending.

Legend: ✔ In place ■ Partial ✘ Not yet

HOW TO READ THIS

Designed = control is modeled in the product and docs. Operated = running in production with evidence over time. Certification (27001 / SOC 2) requires Operated status plus an evidence window; this is a self-assessment, not a certification.