GRC

Evidence Platform

Evidence once, evaluated against every framework



Every step lands in an append-only, hash-chained audit log.

PRODUCT INFO

TECHNICAL DATA SHEET

GRC Evidence Platform

A compliance evidence platform built on one rule: the model reads, the rules decide, a human signs. One uploaded document is evaluated once against every framework the organisation subscribes to, with page-level provenance, gaps and remediation tasks, and an auditor verdict that locks the control.

Verdicts come from versioned, deterministic rules rather than from a model, so a result can be replayed and explained after the fact, and a change of model never changes a past decision. Five parties are supported: an audit firm and its auditors, and an audited organisation with its org admin and control owners.

How It Works

Three parties each do the part they are good at, and nothing blurs the boundary between them. The boundary is what makes a verdict reproducible, resistant to prompt injection, and defensible to an auditor.

MODEL
Extracts facts

- Reads the document (native text first, a vision model only as a fallback)
- Reports what it says, with the quote and page it came from
- Local or remote: Ollama, LM Studio or any OpenAI-compatible endpoint
- Never decides pass or fail

RULES
Decide, deterministically

- Versioned content packs written in YAML
- One document evaluated against every subscribed framework
- Verdict records the rule hash, engine version and inputs
- Replayable: same facts and rules, same verdict

AUDITOR
Signs and locks

- A named human records the verdict
- Locking is enforced in the API and the data layer, not only the UI
- Uploader and verdict-giver can never be the same person
- Reopening is a recorded act with a reason

Audit log underneath

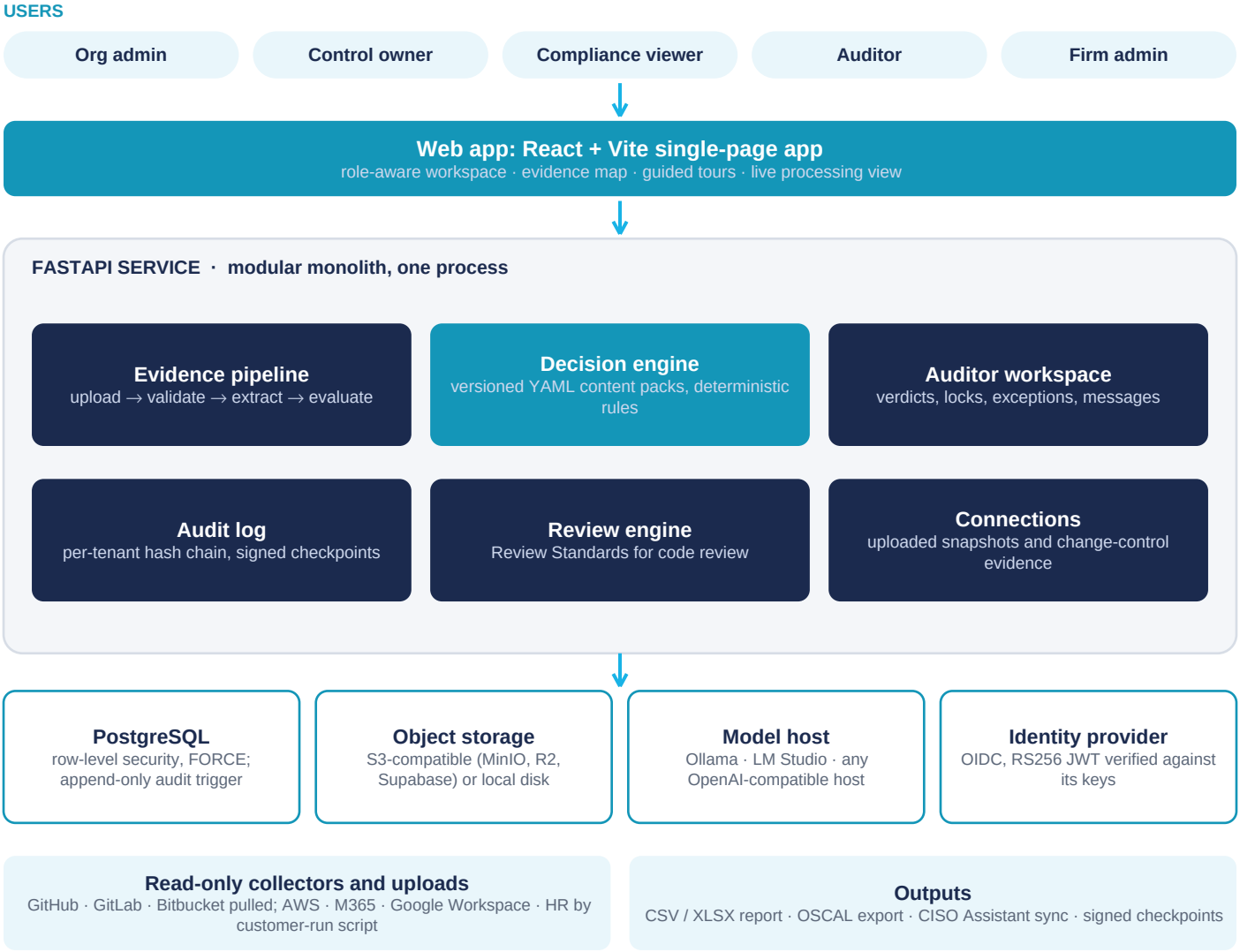
Per-tenant hash chain · database refuses edits and deletes on Postgres · signed checkpoints the auditor keeps · offline verifier

Five Roles, One Workspace

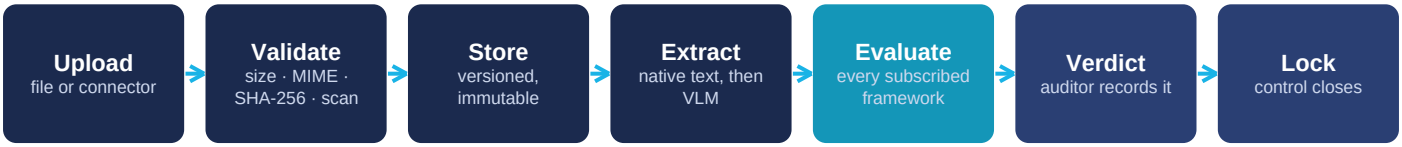
Role	Party and what it does
Org admin	Audited organisation. Uploads evidence, invites owners, registers controls, submits for review
Control owner	Audited organisation. Works assigned tasks, fixes gaps, uploads new versions of evidence
Compliance viewer	Audited organisation. Read-only view of readiness by framework, every gap and the audit trail
Auditor	Audit firm. Records verdicts, locks controls, requests evidence; scoped to engaged frameworks only
Firm admin	Audit firm. Approves onboarding, staffs auditors, tracks every client, opens an engagement

Belonging to a firm grants access to nothing. Being staffed on an engagement is the grant, and an unstaffed client answers 404, indistinguishable from one that does not exist.

System Architecture



Evidence Lifecycle



Status shown to the user: STORED · EXTRACTING · ANALYZING · EVALUATING · READY · NEEDS_REVIEW · FAILED

A new version supersedes the old one and resolves the gaps it fixes; the old version's gaps and verdicts stay on record. If the model is unavailable the file is stored and flagged, never silently passed.

Modules & Features

Module	Key highlights
Evidence & Extraction	• Upload with validation: size, name, MIME sniffing, allowlist, SHA-256, malware-scan hook • Versions supersede, never overwrite; soft delete keeps history • Page-level provenance for every extracted fact; quality and freshness scoring • Live processing view while a document is analysed
Compliance Engine	• Nine content packs: ISO/IEC 27001:2022, PCI DSS 4.0.1, SOC 2, HIPAA Security Rule, GDPR, DPDP 2023, NIST CSF 2.0, NIST AI RMF 1.0, CIS Controls v8 • Unified control objectives (25) so one fact satisfies several frameworks • 93 of 93 ISO 27001 Annex A controls and 33 of 33 SOC 2 Security criteria are listed; a requirement with no rule yet is met by a named person's dated attestation, shown as Attested, never as passed • Gaps carry the exact missing or short attribute and what to fix • Draft requirements from a law's own text (parsed deterministically), with a human review gate and an advisory model critique
Controls, Gaps & Tasks	• Per-control verdicts, remediation tasks created from gaps, manual tasks and priorities • Auditor and auditee message threads: evidence requests, unlock requests, comments • Group tasks by the fix they share; assign, schedule and re-prioritise many at once • Control owners added and removed from the control page, optionally handing over open tasks • Notifications for expiring and expired evidence
Auditor Workspace	• Verdicts that lock a control; reopening needs a stated reason • Segregation of duties enforced, not assumed • Signed audit-chain checkpoints (Ed25519) held by the auditor, verifiable offline • Verdict provenance: rule hash, engine version, inputs, Replay • Verdict history that is never edited: replacing a verdict adds a reopening and the new decision, each with its reason • Findings: an auditor raises one, the auditee responds, the auditor closes it; every step is audited • Overriding the rules' own verdict needs a stated reason
Gap Exceptions	• Time-bound (180 days at most), approved by an auditor, never by the requester • Bound to the rule and the gap value: a changed rule or a bigger gap retires the exception • Computed at read time, so no scheduler is needed to expire one
Connectors & Change Control	• AWS, Microsoft 365, Google Workspace and HR-leaver evidence comes from the customer's own read-only script, as yes/no answers uploaded with a token: we hold no cloud keys. A snapshot counts for 30 days, and a weekly GitHub Actions template runs them • GitHub, GitLab and Bitbucket change control, pulled with a token the organisation saves encrypted • Pre-merge change-control gate that runs the audit's own rules in CI • Every run recorded as complete, partial or failed; a partial run is never read as a pass • AI code review recorded as evidence, never as approval
Privacy & AI Governance	• DPDP readiness, breach events and data-subject request log • NIST AI RMF starter pack, AI policy and inventory artefact types • Auditor-only AI summaries, clearly labelled as narration
Reporting & Integration	• Compliance report as CSV or XLSX; OSCAL export; a weekly compliance report from what is already stored • CISO Assistant sync of verdicts • Optional webhook notices (Slack, Discord or your own endpoint) and a de-duplicated daily digest • Ask AI: a helper that answers from stored data with read-only tools • Evidence map, activity feed, glossary and guided tours

Running the Programme

Beyond the audit loop, the boundary holds: where a number or a grade is produced (a risk score, a vendor tier, a training result), fixed rules produce it and a person signs. A model may suggest wording, never a score.

Area	What it does
Policy library	• An admin writes and approves each version; every person accepts it for themselves • Editing the text is a new version that everyone accepts again; archiving keeps every version and acceptance • Templates whose figures already meet the frameworks' rules (ADR-038, ADR-056)
Training	• Courses with lessons and graded scenario questions; fixed rules grade them, and the right answer and its reason appear after you answer • Best try per lesson counts: 80% or more is PASS, 50% or more PARTIAL; it repeats every year • An admin sees everyone's result and who is behind; every try is kept. A pass shows a person was given the material and answered, not that they are competent (ADR-063, ADR-064)
Risk register	• A fixed five-by-five scale scores each risk; a person signs; heat map, treatment, owner and next review date • A model may suggest wording and never sets a score (ADR-057)
Vendors	• A register with a rule-decided risk tier from data access, criticality and attestation • A current SOC 2 or ISO 27001 report on file lowers the tier only while its valid-until date has not passed (ADR-042, ADR-043)
Trust page and questionnaires	• A public trust page, off by default and content-free (ADR-039) • Security questionnaire answers drawn from stored verdicts (ADR-040)
First week and drift	• A first-week checklist read from real data, never hand-ticked • A weekly digest of controls that turned worse and sources that went quiet (ADR-041, ADR-058)
Plans and demo	• Plans set by hand with limits on frameworks and people, a FREE plan, and no payment code; an ended trial is read-only (ADR-054, ADR-062) • A public read-only demo organisation: anyone can look, every change is refused by the server (ADR-062)

Evidence Reuse in Numbers

Computed from the content packs in the repository. The same unified control objective is satisfied once and counted by every framework that maps to it, which is why one document can serve several frameworks.

9	183	80	25	90
frameworks	requirements listed	judged by rules	unified objectives	mappings

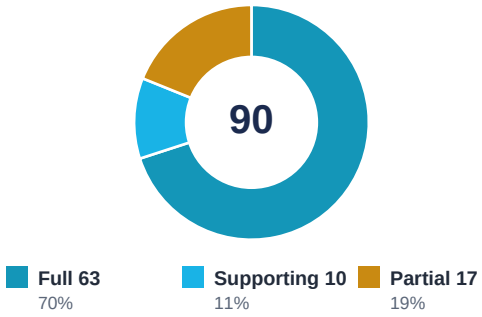
Objectives that reach the most frameworks

frameworks mapping to the objective, out of 9



Mapping coverage

90 mappings, nine packs



Framework × control domain

requirement-to-objective mappings; darker means more

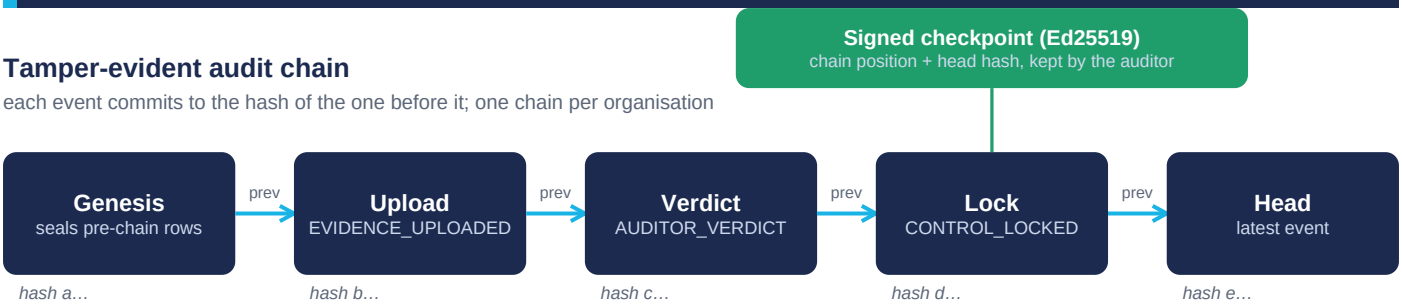
	Rule/all	IAM	Data prot.	Vuln. mgmt	Logging	Change mgmt	Privacy	AI gov.
ISO 27001	12/93	6	1		2	2	2	
SOC 2	11/33	5	1	1	2	2	2	
PCI DSS	13/13	7	1	1	1	2	2	
NIST AI RMF	11/11							11
DPDP	9/9	2	1		1		5	
CIS v8	7/7	5	1	1	1			
NIST CSF	7/7	5	2	1	1			
GDPR	5/5	4	1	1				
HIPAA	5/5	4	1		1			

Reading it: the AI RMF pack maps only to AI governance, while the security frameworks share identity and access, data protection and vulnerability objectives, so the most widely shared objectives reach 7 of the nine frameworks. Every ISO 27001 Annex A control and almost every SOC 2 Security criterion is now listed, but a rule judges only 80 of the 183 requirements; the other 103 are met by a named person's dated attestation until a rule can be written. The mapping counts above are of the 80 rule-judged requirements, as shipped.

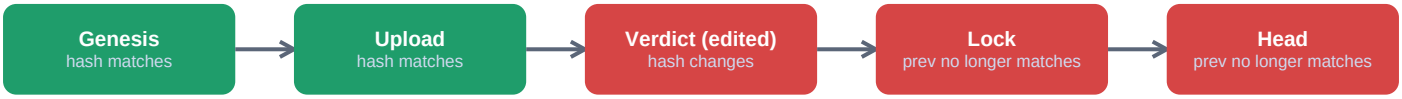
Integrity by Design

Tamper-evident audit chain

each event commits to the hash of the one before it; one chain per organisation



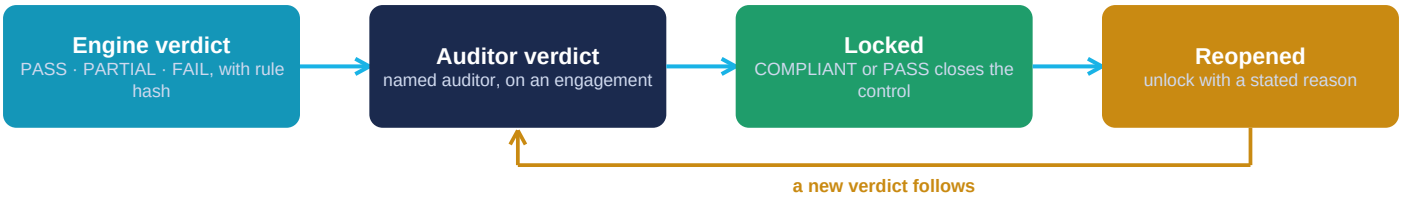
If a past event is edited, inserted or deleted:



Verification fails at the first bad event: "event 3 does not hash to its recorded value". On Postgres a trigger also refuses UPDATE and DELETE.

Control verdict lifecycle

the model never appears here: rules produce the engine verdict, a person records the opinion

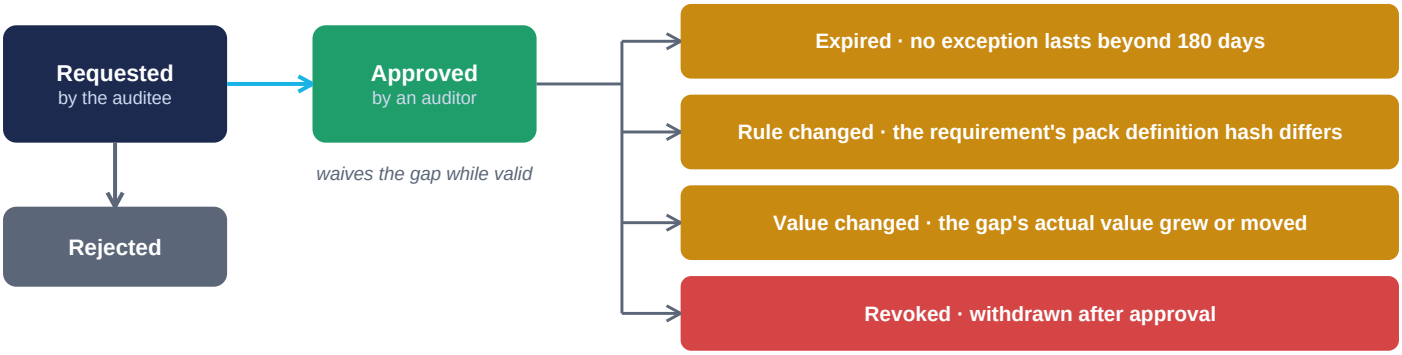


Segregation of duties
the uploader of the evidence cannot record its verdict

Verdict register
every reopening and replacement kept as its own record, with its reason

When a gap exception stops applying

validity is recomputed on every read against the rule and the gap as they are now



Distinctive Features

What sets the platform apart from a document-store GRC tool is that the result is reproducible, attributable and tamper-evident.

Evidence reuse
One document evaluated once against every subscribed framework

Deterministic verdicts
Rules decide; the same inputs give the same result

Replay
Rules a verdict was judged against are kept, so it can be re-run later

Hash-chained audit log
Per-tenant chain; any edit, insert or delete breaks verification

Auditor-held checkpoints
Signed statements of the chain head, verified offline with a script

Expiring exceptions
Waivers lapse on time, on rule change or when the gap grows

Tenant isolation in the DB
Postgres row-level security, forced, not only app filters

Segregation of duties
Uploader cannot judge; exception requester cannot reopen

Your own model
Local, or any OpenAI-compatible host you choose; the model never decides a verdict

Change-control evidence
Collected from GitHub, GitLab and Bitbucket as it happens

Findings workflow
Raised by an auditor, answered by the auditee, closed on the record

Alerts where you work
Optional webhook notices and a daily digest; content-free by design

Platform Security

Authentication	OIDC with RS256 JWT verification against the provider's keys; a production deploy refuses to start without OIDC configured. Multi-factor policy is the identity provider's, not the platform's.
Tenant isolation	Postgres row-level security with FORCE on tenant tables; firm and organisation are separate axes.
Audit integrity	Per-tenant hash chain, database-level append-only trigger on Postgres, Ed25519-signed checkpoints (when a signing key is configured), offline verification script.
Upload handling	Size, filename, MIME sniff, extension agreement, allowlist, SHA-256 and a malware-scan hook (ClamAV supported; the default scanner is a no-op).
Roles and access	Role-based access plus engagement scoping; read-only roles cannot write; unstaffed clients return 404.
Browser and operator	Standard security headers on every response, and a Content-Security-Policy in report-only mode (not yet enforced). Wrong operator keys are limited to ten per address in five minutes (ADR-065, ADR-066).
Supply chain	A weekly scan of known vulnerabilities in what ships (pip-audit, npm audit) and Dependabot update pull requests; every change is a reviewed pull request behind a change-control gate.

Key Benefits

Defensible results	• A verdict names its rules, engine and inputs and can be replayed • The model never decides compliance
Evidence reuse	• One upload satisfies several frameworks and yields precise, per-framework gaps • New versions resolve gaps and keep their history
Audit readiness	• Append-only trail with before and after state and a reason • Auditor-held, signed checkpoints that outlive the platform's own word
Fits regulated work	• Models can run locally or on your own host; storage is S3-compatible or local • Isolated tenants, firm and client axes
Faster remediation	• Gaps become tasks automatically • Auditee and auditor talk inside the control, on the record

Deployment Model

Full stack, one command	docker compose up brings up Postgres, MinIO (S3 storage), Ollama and the API serving the web app.
Managed pilot	A Render blueprint: one web service with managed Postgres and S3-compatible storage (the live pilot uses Supabase for both), the model hosted elsewhere; a separate stub-auth demo service for sharing, with throwaway data.
Your storage, your model	S3-compatible object storage or local disk; Ollama, LM Studio or OpenAI-compatible endpoints.
Scheduled collection	Expiry monitoring and connector sync run from cron, Task Scheduler or CI, and the customer's upload scripts from their own scheduler or a GitHub Actions template; there is no in-process scheduler.

Boundaries — what this sheet does not claim

- 183 requirements are listed across nine frameworks, but a rule judges only 80; the other 103 (most of ISO 27001 and SOC 2) are a named person's attestation, which an auditor judges and the platform does not verify.
- Of SOC 2, 33 of the 33 Security (CC) criteria are listed; the availability, confidentiality, processing-integrity and privacy categories are covered only in part or not at all.
- Encryption at rest, backups and multi-factor sign-in depend on the hosting, storage and identity provider you choose.
- No third-party penetration test or security certification is claimed for the platform itself, and it has not had its own SOC 2 audit.
- The Content-Security-Policy is report-only: it reports violations and blocks nothing yet.
- The hosted pilot runs on free-tier hosting that sleeps when idle (a first request can take about a minute) and carries no uptime promise.
- The default malware scanner is a no-op; run ClamAV to scan uploads.
- Single web instance only: live updates, background uploads and request limits run in-process.
- Model-backed features (extraction, Ask AI, draft review help) need a reachable model. The hosted demo runs without one, so its evidence comes from collector snapshots.
- AWS, M365, Google Workspace and HRMS connectors have no totals to check against; completeness checks apply from the second run.

Who Should Use It?

Audit firms	Run client engagements with staffed auditors, scoped access and verdicts that lock.
Compliance officers	See readiness by framework, every gap and the audit trail, read-only.
Security and IT teams	Collect change-control and cloud evidence; fix gaps through assigned tasks.
AI governance leads	Map AI policy and inventory evidence to NIST AI RMF alongside security frameworks.
Privacy teams	Track DPDP readiness, breach events and data-subject requests.
Engineering leaders	Gate merges on the same change-control rules the audit will apply.

See It In Action

Two demos run. The live service has a read-only demo organisation anyone can look around: every change is refused. A separate demo has one-click personas for each of the five roles, on throwaway data that resets.

1. **Look around, read-only**
   https://grc.blinkedit.me — choose Try the demo on the sign-in page, no account
2. **Play every role**
   https://grc-demo-vu2u.onrender.com — org admin, control owner, compliance viewer, auditor or firm admin
3. **Read the source**
   https://github.com/SatyamSaxena1/GRC — start with the README and docs/adr

The model reads. The rules decide. A human signs.

History is added to, never rewritten.