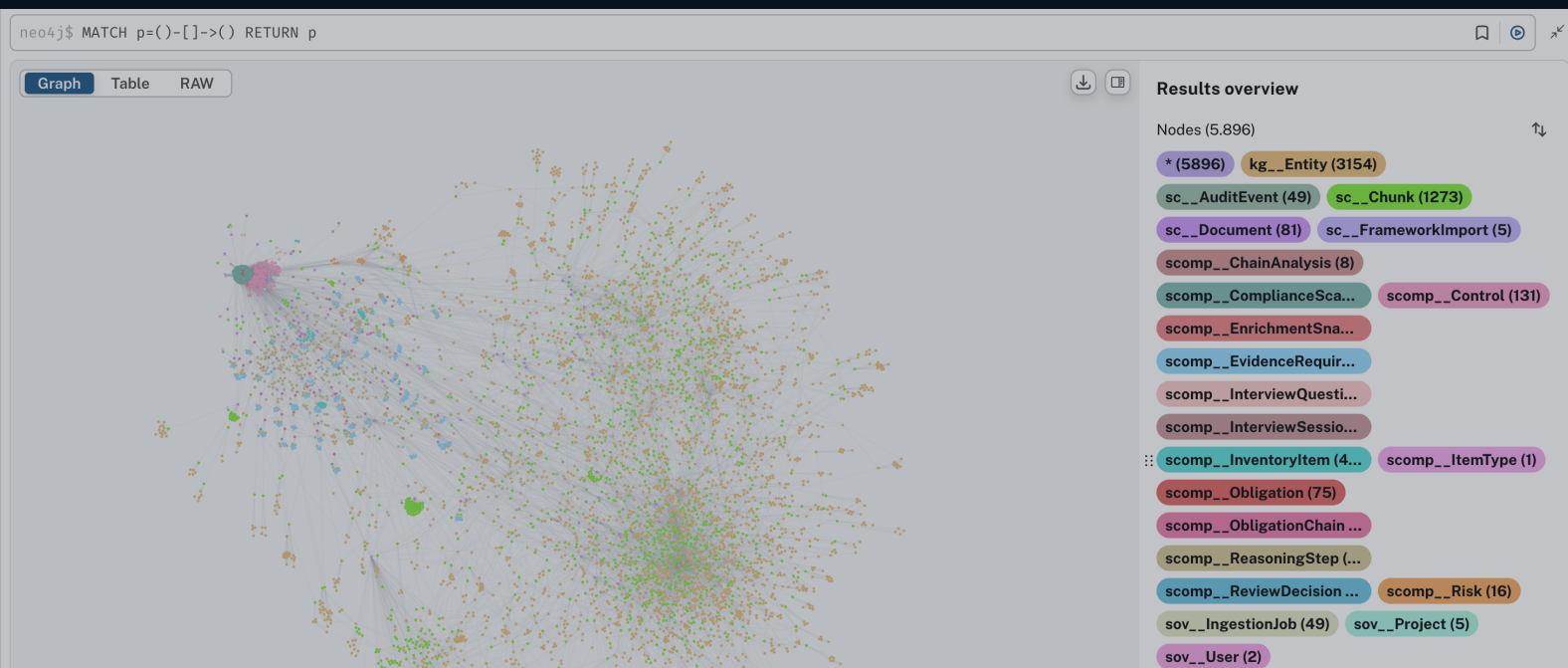


ACCOUNTABILITY INFRASTRUCTURE FOR THE AI AGE

AI. Leveraged to what you commit to.

A compliance knowledge platform that connects your obligations to the evidence, reasoning, and system behaviour that proves you live up to them.



Compliance describes what should happen. Sovaign proves what does.

Most organisations run two separate systems. One for compliance — frameworks, audits, policies. One for operations — data, AI, decisions, infrastructure. Neither talks to the other. Compliance teams spend their time chasing evidence that operations teams didn't know they needed to produce.

Organisations adopting AI are making this gap wider. AI systems make decisions at a scale and pace that traditional oversight was never designed to follow. The obligations created by deploying AI — under frameworks like ISO 42001, NIS2, the EU AI Act — are accumulating faster than the compliance infrastructure to match them.

Sovaign is built to close that gap. It maps your regulatory obligations to the controls, evidence, and system behaviours that demonstrate compliance — and keeps that map current as things change.

Know what you owe

Import frameworks and let Sovaign extract obligations. See immediately what you are required to demonstrate and where the gaps are.

Connect evidence to obligations

Every piece of evidence attaches to a specific obligation through a specific reasoning chain. Nothing floats unaccountably in a document store.

Track freshness, not just coverage

Compliance is not a one-time event. Sovaign flags controls that have gone stale and evidence that no longer meets its obligation.

Audit-ready on request

Point-in-time snapshots mean you can reconstruct your compliance posture at any past date — not just describe it today.

AI that assists without replacing

Sovaign uses AI to surface gaps, draft policies, and suggest evidence — with confidence thresholds you control. Human review stays in the loop.

Runs on your infrastructure

Self-hosted. Your data stays within your boundary. Sensitive compliance content does not leave your infrastructure to be processed by third-party services.

A day in the life of a compliance manager using Sovaign

Sovaign is not a form-filling tool. It is closer to a working partner that keeps track of what you have committed to, what you can prove, and what still needs attention.

- 1 Start at the Action Center**

The Action Center shows pending evidence requirements across all active frameworks, an AI-recommended next action, and the current audit readiness score. It is the daily starting point.
- 2 Review what the Advisor has surfaced**

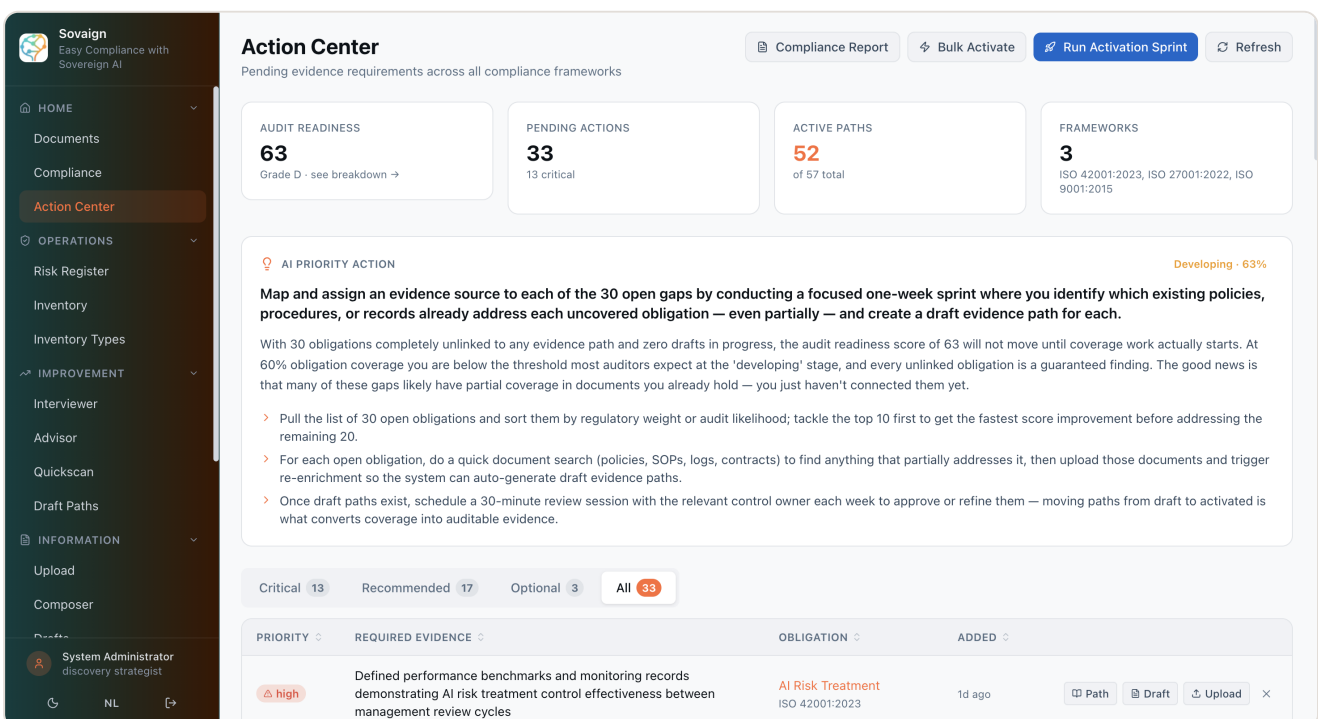
The Compliance Advisor analyses your current graph and produces a frank assessment: what is solid, what is missing, what would fail scrutiny today. No scores — actual reasoning.
- 3 Upload new documents or evidence**

Drop a policy document, a supplier contract, or an audit report into the inbox. Sovaign extracts entities, maps them to obligations, and flags duplicates or superseded versions automatically.
- 4 Check obligation coverage**

The Obligations view shows every requirement from your active frameworks with its current coverage status — fully evidenced, partially covered, or not started.
- 5 Draft a policy or control document**

The Document Composer generates a first draft of a policy or control instruction from your framework context. You review and approve before it enters the graph as active evidence.
- 6 Check the readiness score before a review**

The composite score — evidence coverage, freshness, gap resolution, SLA — gives an honest picture. No single dimension can mask a failure in the others.



Action Center — the daily starting point for a compliance manager

Key screens

Organization
Cross-project compliance overview

Refresh

PROJECTS 9	OBLIGATIONS 82 In Scope: 75 Not Evaluated: 0 Deferred: 0 Excluded: 0	CONTROLS 131 In Scope: 131 Not Evaluated: 0 Deferred: 0 Excluded: 0	EVIDENCE ITEMS 93	AVG COVERAGE 56.4%
AVG SLA COMPLIANCE 100.0%	AVG AUDIT READINESS 69.1% Avg across all projects - see Readiness for single-project score	OVERDUE ACTIVITIES 0 all up to date	GAP SEVERITY CRITICAL 8 projects below threshold	

Overview | Project Comparison | Gap Analysis

Performance Highlights

Recommendations

- Warning: Average evidence coverage is 56.4%. Consider evidence collection sprints for under-covered controls.
- Attention: 8 project(s) below 70.0% coverage threshold: SovaignTestISMS, ddfISMS, ddfvzfvISMS and more.
- Gap detected: 30 obligations have no activated evidence chain. Run hub generation to cover these obligations.

Organisation overview

Executive-level summary across all projects: obligation counts, control inventory, evidence totals, average coverage, SLA compliance, and composite audit readiness. A single view of where the organisation actually stands.

Advisor
Your single most impactful next step, based on current compliance posture

Framework: All Frameworks | Get Recommendation | Refresh

PRACTICE NOTES

Impressive policy architecture, but the actual management system hasn't been built yet.

Your integrated policy document and scope foundations are genuinely strong for a two-person operation. The AI policy specifically — with its named commitments to bias assessment, human oversight, transparency, and logging — is substantive, contextual, and reflects real operational thinking. Certification bodies see a lot of copy-paste AI policies; yours reads like someone who actually runs AI workloads. The Technical Component Inventory, the Context document, and the Stakeholder document give you a credible clause 4 story across all three standards. That is a real foundation. Most two-person shops walk in with nothing.

Now for the audit reality: an ISO 27001 auditor's first three requests will be the risk register, the risk treatment plan, and the Statement of Applicability. You have none of these. Without them, certification is impossible — not difficult, impossible. These are not optional administrative artefacts; they are the structural spine of ISO 27001. The SoA alone determines which of the 93 Annex A controls you claim to apply, and why you've excluded the rest. You've published 131 controls but have no document formally linking them to assessed risks. Meanwhile, every obligation in clauses 6, 7, 8, 9, and 10 is deferred across all three standards — that is not a phased approach, that is the entire operating layer of a management system left unbuilt. For ISO 9001 specifically, you have no quality objectives and no documented QMS process descriptions, which means your quality management system is a policy statement, not a system. Leadership commitment (5.1) is unactivated for all three certifications; the auditor will ask Tobias to demonstrate top management review and direction of the ISMS/AIMS/QMS, and 'one man does everything' will not satisfy a clause that requires documented evidence of active leadership engagement.

The honest PM assessment for a two-person team pursuing three concurrent certifications: you are carrying enormous scope risk. The deferred clauses 6-10 are not peripheral — they represent risk planning, operational controls, performance monitoring, and improvement, the very mechanisms that make a management system

Compliance Advisor

AI-generated assessment of your current compliance posture. The Advisor reads your graph — what is evidenced, what is missing, what is stale — and produces a plain-language account of what would and would not survive an audit today. Confidence thresholds are configurable: conservative, moderate, or aggressive.

Compliance Management

Obligations Scope Management

Framework: All Frameworks Project: All Projects

Search obligations... All 75 Gaps 30 Pending 0 Covered 45 Refresh

OBLIGATION	COVERAGE	PATHS	STATUS	CONFIDENCE
Understanding the organization and its context 4.1 ISO 27001:2022	substantial	1	activated	—
Understanding the organization and its context 4.1 ISO 42001:2023	substantial	1	activated	—
Understanding the organization and its context 4.1 ISO 9001:2015	full	2	activated	—
Understanding the needs and expectations of interested parties 4.2 ISO 42001:2023	substantial	1	activated	—
Understanding the needs and expectations of interested parties 4.2 ISO 9001:2015	substantial	2	activated	—
Understanding the needs and expectations of interested parties 4.2 ISO 27001:2022	full	1	activated	—
Determining the scope of the AI management system 4.3 ISO 42001:2023	substantial	1	activated	—
Determining the scope of the quality management system 4.3 ISO 9001:2015	substantial	1	activated	—
Determining the scope of the information security management system 4.3 ISO 27001:2022	full	1	activated	—

Obligations and coverage

Every requirement from your active frameworks — ISO 27001, ISO 42001, NIS2, EU AI Act, or your own — listed with its current coverage status, evidence linkage, and gap detail. Progress bars show how far each obligation chain has been completed, not just whether it has been touched.

Risk Register

Risks extracted from Risk Register documents and their obligation linkages

+ Extract from Document

Total risks: 16 Open: 16 Mitigated / Accepted: 0 Critical (≥ 0.7): 2

ID	TITLE	CATEGORY	PROB	IMPACT	SEVERITY	TREATMENT	STATUS	OBLIGATIONS	CONTROLS
R-AI-005	AI-Generated Control Statements Published Without Human Review	Operational	High	Critical	Critical (0.90)	Avoid	Open	3	0
R-IS-001	Unauthorised Access to Customer Data via Weak Authentication	Information Security	High	Critical	Critical (0.90)	Mitigate	Open	0	0
R-AI-004	Knowledge Graph Poisoning via Malformed Ingestion Files	Information Security	Medium	Critical	High (0.50)	Mitigate	Open	3	0

Ransomware

Risk Register

Risks tracked with probability, impact, severity, and treatment status. Each risk links to the obligations it is relevant to, so coverage gaps and risk exposure are visible in the same view. Sixteen risk entries in the example above, each with its own treatment and obligation mapping.

Sovaign
Easy Compliance with
Sovereign AI

- HOME
- Documents
- Compliance
- Action Center
- OPERATIONS
- Risk Register
- Inventory
- Inventory Types
- IMPROVEMENT
- Interviewer
- Advisor
- Quickscan
- Draft Paths
- INFORMATION
- Upload
- Composer
- System Administrator
discovery strategist

localhost:3000/framework-quickscan

Quickscan

Clause coverage heatmap and document scan evidence

Framework: All Frameworks
Evidence
Heatmap
Refresh

IN-SCOPE OBLIGATIONS

75

COVERED

45 (60%)

GAPS

30

PENDING

0

Total Scans	Obligations with Evidence	Controls with Evidence	Strong (Obligations)	Strong (Controls)	Refresh
185	75/75	131/131	75	127	

Obligations (75)
Controls (131)

CLAUSE	TITLE	BAND	CONFIDENCE	TOP SOURCE	DOCS
9001.4.1	Understanding the organization and its context	strong	86%	Sovaign_Policy_and_scope_for_quality_information_secu...	16
9001.4.2	Understanding the needs and expectations of inte...	strong	92%	SOVAIGN_STAKEHOLDERS	10
9001.4.3	Determining the scope of the quality management...	strong	87%	iso27001-isms-scope-statement	24
9001.4.4	Quality management system and its processes	strong	88%	Sovaign_Policy_and_scope_for_quality_information_secu...	11
9001.5.1	Leadership and commitment	strong	88%	iso27001-continual-improvement-plan	18
9001.5.2	Policy	strong	85%	iso27001-continual-improvement-plan	17
9001.5.3	Orqanizational roles responsibilities and authorities	strong	88%	iso27001-information-security-policy	20

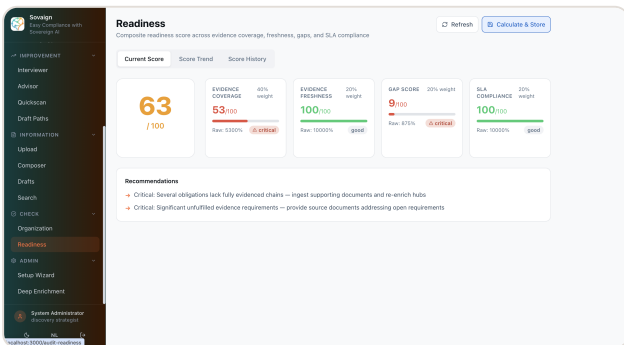
Quick compliance scan

A rapid overview of control coverage: how many controls are active, what percentage have evidence, how many gaps remain, and whether any items are overdue. Useful as a daily check before a meeting or a pre-audit sense-check.

DOCUMENT	STATUS	LABEL	VER.	CREATED	UPDATED	COMPLIANCE SCAN
AI multi-agent architecture	active	all users	v1	14 mrt 2026	14 mrt 2026	Scan Test Match
sovaign-statement-of-applicability-2026 Global	active	all users	v1	12 mrt 2026	—	Scan Test Match
sovaign-staff-awareness-survey-2026 Global	active	all users	v1	12 mrt 2026	—	Scan Test Match
sovaign-risk-register-2026 Global	active	all users	v1	12 mrt 2026	—	Scan Test Match
sovaign-resources-adequacy-determination-2... Global	active	all users	v1	12 mrt 2026	—	Scan Test Match
sovaign-physical-security-inspection-2026 Global	active	all users	v1	12 mrt 2026	—	Scan Test Match
sovaign-phishing-simulation-report-q1-2026 Global	active	all users	v1	12 mrt 2026	—	Scan Test Match
sovaign-person2-awareness-training-record-...	active	all users	v1	12 mrt 2026	—	Scan

Document library

All evidence documents in one place — policies, procedures, supplier agreements, audit reports, survey results. Each document is version-tracked: when an updated version is ingested, the previous version is superseded rather than overwritten, so the history is preserved and auditable.



Audit readiness score

Composite 0–100 score across four weighted dimensions: evidence coverage (40%), evidence freshness (20%), gap resolution (20%), and SLA compliance (20%). Each dimension is visible separately — a strong score in one cannot hide a failure in another.

Management System Setup Wizard
Get from zero to a complete compliance posture in under 5 minutes

Tell us about your organization
This information will be used to personalize your Management System and pre-fill policy templates.

Company Name *
e.g. Acme Corporation

Industry
Select industry (optional)

Management System Scope Statement *
e.g. All information systems within the HQ data centre and supporting cloud services used for processing customer data.

Describe what is covered by your Management System. This maps to clause 4.3 of your selected framework(s).

Project Name *
e.g. AcmeMS
Alphanumeric name used to scope this Management System in the graph.

[Create Project](#)

Getting started: the setup wizard

First-time setup walks through company information, framework selection, and initial document ingestion. New frameworks can be added at any time, and the obligation extraction runs automatically on import.

Everything connects. Nothing gets lost.

Sovaign stores all compliance knowledge in a Neo4j graph database. Obligations, controls, evidence, documents, assets, and risks are nodes. The relationships between them — who owns what, what proves what, what supersedes what — are first-class data. You can search the full graph, trace any piece of evidence back to the obligation it satisfies, or run arbitrary Cypher queries for custom analysis.

The screenshot shows a Neo4j web interface. At the top, a Cypher query is entered: `neo4j$ MATCH p()-[]->() RETURN p`. Below the query bar are tabs for 'Graph', 'Table', and 'RAW'. The main area displays a large, dense network graph with nodes of various colors (pink, blue, yellow, orange) and connecting lines. On the right side, there is a 'Node details' panel for a selected node of type 'sc__Document'. The panel contains a table of key-value pairs:

Key	Value
<id>	4:e23c51e3-8b23-4a2f-b0ec-6964ed703f92:1160
schema_ns	"discover"
status_history	["active"]
created_at	2026-02-17T23:32:30.39400000+01:00[Europe/Amsterdam]
project	"Global"
version_notes	"Version 1 - Initial version"
source	"ingestion_pipeline"
title	"SOVAIGN_STAKEHOLDERS"
uri	"urn:sovaign:document:a2d6f1d4e66bc8eab873ce7d7b4393ec0fe8bf326e80e4e429ecdd8df3f9c588"
created_by	"node-red"
version	1
content	"SOVAIGN STAKEHOLDERS 2026-01-25"

At the bottom right of the interface, a status message reads: 'Started streaming 2676 records in less than 1ms and completed after 586 ms.'

The Sovaign knowledge graph — obligations, controls, evidence, and relationships in a single queryable structure

Ready to take a look?

Sovaign is currently in early access. If you are a compliance team, an MSSP, or an organisation deploying AI under regulatory obligations, we are keen to talk.

sovaign.com · app.sovaign.com