

Kautilix Compliance Manager

ISO 27001 readiness, evidenced.



AI-assisted evidence review for teams preparing for certification, customer security reviews and internal audit.

The problem

Most organisations discover their compliance gaps in the audit room. Evidence sits scattered across policies, SOPs, access reviews, risk registers, training records, tickets and meeting minutes, and no one can say with confidence which controls have real proof behind them.

A policy is not evidence of operation. A control needs the policy, the implementation record, and recent operational proof — a single uploaded PDF satisfies none of that. Generic AI document search makes this worse, not better: it will confidently summarise a policy as though the control were operating.

Built for

Auditee-side teams, not auditors. CISOs, ISMS managers, and internal audit and compliance functions at startups and mid-market organisations pursuing ISO 27001 or ISO 42001 — and the security consulting partners who run their gap assessments and want to cover more clients per consultant.

Why it is different

Three design decisions separate Compliance Manager from generic AI document search.

01

Deterministic rule layer

Expiry dates, retention periods, review frequencies, counts and thresholds are resolved in code, with no model involved — removing the LLM from precisely the tasks it is weakest at.

02

Citation validator

Every claim is checked against the evidence actually supplied. A verdict citing nothing — or citing something never provided — is downgraded for review, not shipped.

03

Evidence adequacy gate

When the retrieved evidence is too thin to support a verdict, the system declines to ask the model at all. That is the condition that produces confident hallucinations.

Every control returns a cited verdict: Ready · Partially Ready · Not Ready · Missing Evidence · Not Applicable · Review Required

How it works

1

Upload

The control set and whatever evidence you already hold — no data-store integration first.

2

Structure

Each control becomes a typed, checkable requirement rather than a paragraph of prose.

3

Retrieve

Hybrid keyword and semantic search surfaces candidate evidence, re-ranked for relevance.

4

Validate

Rules resolve what is mechanically checkable; the model is asked only where judgement is genuinely needed.

5

Report

Cited verdicts, a readiness scorecard, a gap register, and a full audit trail.

What you get

Framework packs

ISO 27001 Annex A controls plus the Clause 4–10 management-system requirements. ISO 42001, custom internal control sets and customer security questionnaires run on the same mechanism.

Structured evidence taxonomy

Policy, procedure, record, log, register, screenshot, interview response and external certificate — so “we have a policy” stays distinguishable from “we can prove we operate it”.

Hybrid retrieval

Keyword and semantic search combined, with LLM re-ranking to strip low-relevance noise before any verdict is formed.

Readiness scorecards

Per-control results rolled up by control family and overall, so remediation effort goes where the exposure actually is.

CAPA register

Every gap becomes an owned, dated, retestable action with a severity and a status lifecycle — not a line in a spreadsheet nobody revisits.

Statement of Applicability assistant

Proposes an applicability decision and justification for each Annex A control, for human confirmation rather than silent auto-generation.

Interview mode

Asks targeted questions where documentary evidence is thin, and marks the answers unverified until a document is attached to back them.

Complete audit bundle

Input file hashes, configuration snapshot and a full record of every model call — so any verdict can be reconstructed and defended months later.

What it changes

- Gaps surfaced weeks before an auditor finds them, not during the audit.
- Audit preparation compressed from weeks of manual mapping to days of review.
- A defensible per-control evidence trail that survives auditor challenge.
- Quarterly readiness checks in place of an annual fire drill.
- For consulting partners: materially more client coverage per consultant.

Live in 1–3 weeks

No identity, catalogue or data-store integration is required before you get value. Upload the control set and the evidence corpus, and it runs. Deeper integration with document repositories and ticketing systems is available — but it is not a precondition for the first assessment.

Where it goes next

ISO 42001 readiness as the second framework pack, positioning the product for AI-governance readiness in AI-native and AI-adopting organisations · customer security questionnaires and vendor due-diligence assessments as further packs on the same engine · periodic re-assessment with evidence versioning and change tracking, so readiness becomes a monitored state rather than a point-in-time exercise · multi-entity dashboards for consulting partners and group compliance functions.

Compliance Manager supports audit preparation and internal review. It does not make certification decisions, and it is not a substitute for an accredited audit. Every verdict is cited, reviewable, and designed for human confirmation.

Readiness scorecards, the CAPA register, the Statement of Applicability assistant and interview mode are in active development. The underlying evidence-review engine — deterministic rule layer, citation validator, adequacy gate, hybrid retrieval and audit bundle — is in production today.

See it run against your own control set.

info@tattvasit.com
tattvasit.com