Axel Hoehnke
Virtual CISO · Governance Advisor · EU Cybersecurity Specialist

Case Study: ISO 27001 Stage 2 Certification

Legal AI Technology Company — Switzerland

SECTOR	SIZE	LOCATION
Legal technology / AI software	Scale-up, ~50–100 employees	Zürich, Switzerland
ENGAGEMENT	**DURATION**	**DELIVERED**
ISO 27001:2022 Stage 2 — Readiness Bootcamp + Live Audit Support	Two weeks	September 2025

The Situation

A Legal AI technology company in Zürich had completed its Stage 1 audit — conducted by an accredited external certification body — and was preparing for Stage 2 within weeks. The Head of People & Operations needed two things: a structured preparation sprint to address open findings, and an experienced advisor available to support the team in real time on audit day.

This was not the first engagement. Two years earlier, in a senior operations role at a different company, she had brought me in for an ISO 27001 Stage 1 internal audit on the same Vanta platform. She understood the process and knew what the output needed to look like for an external certification body.

The timeline was fixed. The auditor was already scheduled. There was no room for drift.

What I Did

The engagement ran as a two-week Compliance Sprint, with live support on audit day itself.

Scope — I reviewed the Stage 1 audit report from the British Assessment Bureau in full and mapped every finding against the current state of the Vanta ISMS. We agreed a written bootcamp plan: which gaps to close, in which order, by which date, and who owned each item.

Baseline — Working directly in the Vanta environment, I assessed the current state of each open control area against ISO 27001:2022 requirements — with particular attention to the Statement of Applicability and the justifications for any excluded Annex A controls.

Gap — Two priority risks emerged. First, physical security: the server and network room was not locked, exposing IT infrastructure to a finding under Clause 7 / Annex A.7.3. Second, SoA governance: several Annex A controls (5.5, 5.12, 5.31, 7.8, 7.11, 7.12) had been excluded without sufficient justification.

A third issue emerged mid-sprint: the Management Review Meeting from May 2025 had been documented with minutes that did not reflect the required discussion of interested parties feedback and internal/external factors. The auditor had flagged potential escalation to a Minor — or Major — non-conformity. We resolved it before it became a finding.

Deliver — Two corrective action records were prepared and submitted with full documentation: root cause, immediate actions, procedural changes, responsibility assignments, and target dates. Both were accepted. Certification confirmed within ten days of audit close.

The Results

METRIC	RESULT
Stage 1 findings addressed	100% prior to Stage 2
Non-conformities raised at Stage 2	2 (both minor)
Non-conformities resolved	2 — corrective action records accepted
Management review escalation	Prevented — resolved mid-sprint
Certification outcome	Confirmed — British Assessment Bureau

NC-1 — Clause 7 / Annex A.7.3 (Physical Security): Network cabinet locked immediately. ISMS procedure updated with quarterly access control checks. Office Manager assigned as control owner. Annual physical security re-evaluation added to risk assessment cycle.

NC-2 — Clause 6.1.3 (Risk Treatment / Statement of Applicability): Controls 7.11 and 7.12 reinstated. Evidence remapped in Vanta. SoA Governance Checklist implemented. Dual sign-off process introduced. Quarterly SoA review added to ISMS calendar.

What the Client Said

> *“Thank you Axel — everything worked out. We should receive the report within the next ten days. I’ll let you know as soon as the certification is finally confirmed — but it looks good.”*
>
> **— Head of People & Operations, Legal AI Technology Company, Switzerland**
> (Personal reference available upon request)

What Made This Engagement Different

This was a live certification sprint with a fixed external deadline, real non-conformities to resolve, and an escalating documentation issue handled under pressure in real time. The value was not just in knowing what ISO 27001:2022 requires — it was in knowing how certification auditors think, which issues escalate, and how to document corrective actions that close a finding for good rather than patching it for one audit cycle.

The returning client relationship reflects something beyond competence: when an operations leader moves to a new company and brings the same advisor with her, it signals trust in the process and confidence in the output.

Relevant for Your Organisation If:

- You are preparing for ISO 27001 Stage 2 and your Stage 1 report has open findings
- Your Vanta ISMS has controls excluded in the SoA that may not withstand auditor scrutiny
- You need a structured two-week sprint — not an open-ended advisory engagement
- You want an advisor available on audit day, not just in the weeks before it
- Your certification body is already scheduled and the timeline is fixed