A

Axel Hoehnke

Virtual CISO · Governance Advisor · EU Cybersecurity Specialist

Case Study: ISO 27001 Internal Audit

Medical Diagnostics Provider — Healthcare Sector, Austria

SECTOR	**SIZE**	**LOCATION**
Medical diagnostics / Pharma	Scale-up, ~30–50 employees	Austria
ENGAGEMENT	**DURATION**	**DELIVERED**
ISO 27001:2022 Internal Audit (Stage 1 prep)	Two weeks	July 2025

The Situation

A medical diagnostics company specialising in protein analysis for the pharmaceutical industry and clinical diagnostics was preparing for its ISO 27001:2022 external Stage 2 certification audit. The company had already implemented its ISMS the previous year and needed an independent internal audit to verify compliance, identify any remaining gaps, and produce an evidence-ready report the external auditor would see.

The CIO had one clear requirement: a structured, transparent process that produced a defensible audit record — not a formal exercise that added friction without adding value.

What I Did

The engagement ran as a two-week Compliance Sprint, structured across four phases.

Scope — I confirmed the audit scope against the prior year's Statement of Applicability. No changes to scope were needed. All in-scope information assets, departments, and applicable controls were documented before the audit began.

Baseline — I was granted read-only access to the company's Vanta GRC environment as an authorised internal auditor. Rather than relying on self-reported status, I reviewed each control directly in the platform — policies, evidence attachments, automation test results, and asset configurations — against the Statement of Applicability as a working document.

Gap — I identified exactly which controls had evidence gaps and where risks existed. Every finding was mapped to a specific ISO 27001:2022 control. No finding was raised without a corresponding obligation. I assessed risk implications directly with the CIO: where deviations existed, we discussed whether risks were present and whether existing compensating controls already addressed them.

Deliver — The final audit report was delivered on day fourteen. It contained a structured findings summary, positive observations, corrective action requests with assigned owners and deadlines, and agreed countermeasures. The report was uploaded directly to Vanta, making it visible to the external auditor with a timestamped audit trail demonstrating process continuity.

The Results

METRIC	RESULT
Controls assigned	100%
Controls fully completed	85%
Evidence gaps identified	15 specific items
Corrective action deadline agreed	August 1, 2025
Audit report delivered	Day 14
External auditor visibility	Immediate — via Vanta

Strengths confirmed: Role-based access rights correctly enforced, network segregation well-executed, the “need to know” principle applied consistently, and admin rights appropriately restricted to a small, well-managed group. Document quality across the ISMS was consistent and audit-ready.

Gaps addressed: Fifteen specific items identified across business continuity testing, development and QA procedures, container vulnerability management, and management review documentation. Each assigned an owner, agreed countermeasure, and deadline.

What the CEO Said

> *“I would like to express my sincere appreciation and gratitude to Axel for the excellent work he did in our recent internal ISO 27001 audit. His structured approach was clearly noticeable from start to finish and contributed significantly to ensuring the entire process ran smoothly and efficiently.*

> *I was particularly impressed by Axel’s pragmatic and honest manner. At a time when other internal audits often try to extract the maximum for themselves, Axel focused on creating maximum value for us. This attitude not only strengthened trust in the audit process, but also led to tangible improvements and valuable insights for our company.*
>
> *Axel’s ability to communicate clearly and his transparent methods helped ensure that the audit was not just a formal duty, but a genuine opportunity for further development and optimisation of our processes.”*
>
> **— CEO, Medical Diagnostics Provider, Austria**

What Happened Next

The engagement led directly to a six-month Virtual CISO retainer covering ISO 27001 ongoing compliance, NIS2 readiness, and ISO 42001 preparation. The company operates in a healthcare context where NIS2 essential entity obligations, ISO 13485 quality management, and CRA supply chain requirements will continue to converge.

Relevant for Your Organisation If:

- You are in healthcare, pharmaceuticals, or medical diagnostics
- You have an ISMS in progress and need an independent internal audit before your Stage 2
- You are using Vanta and want an auditor with direct platform access
- You need audit output that serves technical teams, leadership, and external auditors simultaneously
- You want a fixed-scope, fixed-timeline engagement — not open-ended advisory

axelhoehnke.com · meet@axelhoehnke.com · NIS2 · ISO 27001 · ISO 42001 · EU Cyber Resilience Act · Engagement details anonymised at client request