July 31, 2026

CASE STUDY INTERNAL AUDIT ISO27001

Transitioning to ISO/IEC 27001: Overcoming Internal Audit Bottlenecks

Prepared by:

Aegentra Information Security & Compliance Team

Aegentra

July, 31, 2026

0
NONCONFORMITIES RAISED

73
LINES OF ENQUIRY TESTED

47
ANNEX A CONTROLS SAMPLED

4 Days
TO FINAL REPORT

THE CLIENT

A small Australian technology company, certified to ISO/IEC 27001:2022, operating with a lean team and a compliance-
automation platform, and approaching its first surveillance audit.

THECHALLENGE

Clause 9.2 requires internal audits conducted by auditors who are objective and impartial. A small organisation cannot easily
satisfy that in-house: the people who designed and operate the management system are the same people who would audit it. The
audit also had to be reported within a narrow window, so the results were available as evidence for the certification body and as
an input to management review.

www.aegentra.com.au

July, 31, 2026

OUR APPROACH

• Fixed fee, with the audit plan, criteria and sampling rationale agreed before fieldwork began.

• A documented two-year audit programme, so the controls sampled this cycle and those scheduled for the next together achieve full coverage across the certification cycle — a point certification bodies routinely test.

• Fieldwork led by a certified ISO 27001 Lead Auditor (CISA, CISM), with engagement oversight and report issue by a certified ISO 27001 Lead Implementer — independent of the design and operation of the management system.

• Evidence obtained by interview, inspection of documented information, examination of records and configuration, and sampling of operational records — every item indexed and retained in the working papers.

• Matters raised during fieldwork were tested against the organisation's evidence before being reported, rather than carried into the report unexamined.

Aegentra

July, 31, 2026

THEOUTCOME

The audit covered all requirements of Clauses 4 to 10 and a risk-based sample of 47 Annex A controls, across 73 lines of
enquiry. No nonconformities were identified. Five opportunities for improvement were recorded, and the previous certification
audit's findings were verified as closed.
Two matters initially raised as potential nonconformities were examined further and closed on evidence, and reported
transparently as such with the reasoning recorded in the working papers.
An interim summary was issued before the surveillance audit began, giving the organisation a written position for its
certification body on day one. The final report followed within four business days of the closing meeting.

WHY IT MATTERS

An internal audit is not a formality. Done properly it gives management real assurance, produces evidence a certification body
can rely on, and surfaces improvements while there is still time to act.

www.aegentra.com.au

contact@aegentra.com.au