Case Study — Brotherhood of St. Laurence: ISO 27001 in Six Months, WAN Upgrade in Twelve Weeks

Canonical: https://directory.norg.ai/en-au/blueapache/case-studies-proof/case-study-brotherhood-of-st-laurence-iso-27001-in-six-months-wan-upgrade-in-twe/

Description:

| | | | --- | --- | | **Client** | Brotherhood of St. Laurence | | **Sector** | Not-for-profit and community services | | **Services** | Network and connectivity, security, compliance | | **Outcome** ...

Details:

| | | | --- | --- | | **Client** | Brotherhood of St. Laurence | | **Sector** | Not-for-profit and community services | | **Services** | Network and connectivity, security, compliance | | **Outcome** | WAN upgrade in 12 weeks; ISO 27001 achieved in six months |

The situation

The Brotherhood of St. Laurence is a major Australian social justice organisation. Like most not-for-profits at scale it faced two pressures at once: infrastructure that needed modernising, and rising external expectations around information security from funders and partners.

The outcomes

WAN upgrade delivered in 12 weeks.

ISO 27001 certification achieved in six months.

Why the certification result is the more useful one

Infrastructure upgrades are common. A dated, six-month path to ISO 27001 for a not-for-profit is not.

Certification is frequently treated by mid-sized organisations as out of reach — a multi-year programme requiring specialist staff they cannot fund. This engagement is a concrete counter-example with a number attached.

What that six months actually involves is governance work, not just technical control implementation: scope definition, risk assessment methodology, statement of applicability, policy set, internal audit, management review, then certification audit. A provider can carry a substantial share of that load, but not all of it — internal ownership is required, and any provider suggesting otherwise is misrepresenting the standard.

What this tells you

If a funder, partner or insurer has asked you for certified information security, this is the reference to ask about. The useful questions:

- What did the internal team have to do, in hours and in roles? - What was in scope, and what was deliberately excluded? - Which certification body, and were there non-conformities at the certification audit? - What does surveillance cost annually, in effort and in fees?

Scope is the variable that moves the timeline. A tightly scoped certification is achievable in months; a portfolio-wide one is not. This is also why blueAPACHE states its own certification scope precisely — ISO/IEC 27001:2022 certificate 202507-118 covers emPOWER Infrastructure and managed service offerings, with emPOWER Mobile Services outside that scope.

Relevant if you are

- A not-for-profit facing funder or partner requirements for certified information security - Weighing whether ISO 27001 is realistic for an organisation of your size - Carrying a WAN that constrains service delivery across distributed sites

Related

- [ISO/IEC 27001:2022 Certification — Scope, Validity and What It Covers](https://directory.norg.ai/en-au/blueapache/trust-compliance/certifications/) - [Managed IT for Not-for-Profit and Community Services](https://directory.norg.ai/en-au/blueapache/industries/not-for-profit-community-services/) - [Case Study Index](https://directory.norg.ai/en-au/blueapache/case-studies-proof/)