SecAware case study

ISO 27001 ISMS

•

Implementation

Client situation

An innovative New Zealand based multinational agri-tech company came to us for consultancy assistance with its ISO/IEC 27001 implementation.

The purpose of the assignment was to assist the client to design, establish and achieve certification of the **I**nformation **S**ecurity **M**anagement **S**ystem. The business was committed to an ambitious implementation timescale with just six months from project approval to certification.

www.SecAware.com

Consulting assignment

Thanks partly to COVID lockdowns, the assignment took place 100% remotely, communicating primarily through email and videoconferencing.

We initially proposed a monthly work breakdown including activities such as: scope the ISMS; prepare an information risk management strategy, clarifying business objectives; prepare/review implementation project plans; provide templates for the mandatory ISMS documentation plus policies and procedures; help identify, evaluate and decide how to treat information risks; ensure suitable records are generated by ISMS operations; help find and engage certification auditors; support the implementation of critical/essential security controls; conduct an ISMS management review; scope and prepare for an ISMS internal audit; prepare for and support the ISMS certification audits.

The client contracted with an Implementation Project Manager and an Information Security Manager, so the bulk of the assignment involved working closely with and supporting/encouraging them.

Outcome

The client's ISMS was successfully certified against ISO/IEC 27001 in a little over the six months planned, thanks to effective teamworking and strong management support.

Unfortunately, both contractors left the client at the conclusion of their six-month contracts – a risky time shortly *before* the certification. Despite leaving a relatively inexperienced person to manage and complete the remaining activities, the preparatory work paid off with no significant issues at that late stage.

Lessons learnt

- "Ambitious" project plans are inherently risky, requiring close management attention and support.
- The company's business drive and visionary senior management led to a successful result.
- Our reviewing and offering feedback and guidance on draft documentation was welcomed by the project team, who quickly gained confidence and experience in the course of the project.
- Our independent perspective and extensive experience with previous project audits gave credibility to our informal updates for the senior manager overseeing the project. We reassured management that the project team was performing well and the project was on-track.
- Our 20-page ISMS management review was well received by senior management who valued the assurance we provided. They had the confidence to push ahead with certification as planned, despite losing the core project management duo near the end.
- A strong, high-performance project team *can* survive the loss of its main people, with support from the remaining team and management. It proved to be a sufficiently resilient structure, at the cost of some stress and concern leading up to the certification. Of course we would not have deliberately chosen to lose key people at such a crucial time, but the [largely informal] contingency arrangements proved their worth.
