SecAware case study

ISO 27001 ISMS

•

Internal Audit

Client situation

Having unfortunately lost its ISO/IEC 27001 certification due to substantial non-conformities (a 'systemic breakdown' according to the certification body), a CISO came to us initially for help to reboot the company's ISMS.

Management had made changes, not least appointing a new CISO to lead the work. The primary purpose of the ISMS is to protect customers' information, while certification is important for customer trust.

Initial discussions with the CISO indicated that the company was quite capable of redesigning and rebuilding its ISMS with little more than gentle encouragement from us, so we agreed on an alternative approach. An internal audit of the ISMS would provide valuable management assurance that everything was in place prior to the planned recertification.

www.SecAware.com

Consulting assignment

The client agreed our proposal and workplan for an ISMS internal audit. The scope was to audit the mandatory requirements of ISO/IEC 27001:2013 *i.e.* the main body clauses rather than the information security controls in Annex A.

The audit findings were generally positive and supportive of the work that had been achieved to rebuild the ISMS. Aside from one major nonconformity (readily resolved), there were just a few minor nonconformities and some improvement opportunities to report and discuss with management.

While being careful to maintain independence, we were pleased to offer gentle mentoring/encouragement to the CISO throughout this assignment. We prepared a brief awareness guide on how to interact with the certification auditors, and suggested clarifying the CISO's accountabilities.

Outcome

The client's certification audit went smoothly with only minor issues, and the company was successfully re-certified. With that pressure lifted, the company is pursuing strategic opportunities to improve its management of information risk and security, exploit the brand value of its certification, and working on security metrics.

Lessons learnt

- ISO/IEC 27001 re-certification is not a foregone conclusion: an ISMS needs to be actively maintained and supported by management in order to remain true to the ISO standard, and aligned with the business.
- An inappropriate choice of ISMS support tool and inadequate management support can degrade the value of the ISMS to the point that it may fail the business.
- Aside from conformity to the standard, an *effective* ISMS supports and enables the business to grow, whereas an *ineffective* ISMS can be costly and set things back.
- Our professional services contract needs to be crystal-clear on accountability for any subsequent changes required *e.g.* date extensions, scope modifications and follow-up work.
- It is hard for us to step back from an organisation facing risks and opportunities, leaving them to their fate rather than continuing to guide and advise. However, it is the client's business, not ours, and maintaining our independence is essential for audit purposes.

Find out more about us on the SecAware and IsecT websites. Read about ISO/IEC 27001 and the other ISO27k standards at www.ISO27001security.com. Email us at info@isect.com.

IsecT Limited, Castle Peak, 1262 Taihape Road, Hastings, New Zealand

Call/text +64 21 16 55 33 5 during NZ office hours