ISO 27001 – A TALE OF A SMALL COMPANY'S JOURNEY TO CERTIFICATION

AHMED ELASHMAWY – Consulting Practice Lead and
TERRY CHAPMAN – Managing Director – *Axenic Ltd*

To certify or not to certify, that is the question

International Standard Organisation certifications can be quite an undertaking for organisations. Whether an organisation decides to adopt an ISO standard only, proceed with certification or do nothing in this space could be a difficult call. In this article, we will walk you through our own journey to certification as we have recently experienced it at Axenic.

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements consists of seven main clauses detailing the requirements for going through a Plan, Do, Check, Act (P-D-C-A) cycle to manage information security risks. The following sections provide a high-level overview of how we approached it.

Leadership and Commitment

Despite being an information security consultancy that have consistently helped clients create and maintain Information Security Management Systems (ISMS) in accordance with the requirements of ISO/IEC 27001:2013 all the way to certification, it took us few years to build and certify our own. The main reason behind that is the resource commitment. Client work has always trumped internal initiatives, so every time we started establishing our own ISMS, it was interrupted by client work. When the business committed capable resources to deliver the ISMS and managed it as it would manage any client work, we started knocking off the requirements one after the other. Formal resource allocation also served as an essential artefact required to evidence clause 5.1 of the standard (Leadership and Commitment) and clause 7.1 (Resources). Having only two policies (Information Security Policy and Acceptable Use Policy) resulted in a more 'digestible' set of principles and in maintainable documentation.

Operation, Planning (a.k.a. Risk Management) and Context

As the standard adopts a risk-based approach to information security, a logical place to start was to conduct a risk assessment and identify risk treatments. Naturally, a standard risk management framework or methodology was required prior to that. Given that standard risk management methodologies require scope and context (Clause 4), those were documented prior to conducting the risk assessment. As per requirement 6.1.3, the selected risk treatments (controls) were compared to Annex A of the standard to verify that no necessary controls have been omitted. A common misunderstanding (even among some security professionals) is that Annex A is the standard, whereas the standard is outlined in the clauses.

You may be interested in learning more about this by reading **From Chaos to Conformance: A Series on implementing an ISMS** by visiting our blog at www.axenic.co.nz/assurance/from-chaos-to-conformance.

As artefacts to demonstrate risk treatment actions are planned and delivered are required, we produced a risk treatment plan, assigned ownership and deadlines, and reviewed those regularly. As risk treatment milestones where achieved, we produced the relevant evidence and ensured they are properly filed against the controls.

Continued on next page…

Performance Evaluation and Improvement

As monitoring and measurement are key to improvement, the standard outlines a set of requirements for these. Identifying performance measures that are linked to the objectives, as well as regular measurement, and management reviews are corner stones to improvement. A formal agenda for management meetings, calendar bookings and formal meeting minutes to document outcomes and decisions, provide sufficient evidence that the organisation is meeting the requirements of this section of the standard. An improvement log to track improvement opportunities, non-conformities and corrective actions helped us track these and ensure the process is effective and evidenced. Finally, the review of a dashboard mapping objectives outlined in the scope and context to specific Key Performance Indicators (KPIs) was always a standard agenda item in any ISMS review meeting.

Once all of the above are in place, conducting an internal audit in accordance with the requirements outlined in 9.2 (Internal Audit) highlighted any gaps we missed and helped us rehearse the external audit. While having a super competent, independent and certified ISO 27001 Lead Auditor was handy, having a capable external party conduct the internal audit on your organisation's behalf should satisfy the standard's internal audit requirement.

The good, the bad and the ugly

We learnt a number of valuable lessons throughout our certification journey. The ISO 27001 certification provides a competitive advantage for most organisations that need to demonstrate secure practices and that would typically be enough motivation to complete the certification itself. However, the implementation of an ISMS in accordance with ISO 27001 requirements provides almost all organisations with significant benefits as it helps mature a number of business processes. It is also important to be realistic about the time required to build and operate an ISMS. Buying templates and forging an ISMS can easily end up being a very expensive failure. When audit time comes, it pays off to be well prepared. We went into audit sessions (both internal and external) with all our evidence open on laptops and ready to show to the auditors without even browsing to the relevant library. Flipping through tabs or windows fluently during an audit definitely inspires confidence.

Even as professionals with track records of getting other organisations to certification, our own experience was not exactly a breeze. Building our own ISMS was more expensive than we expected as we initially tried to perfect every single aspect of it. It was also continually tempting to expand the remit of the ISMS to cover non-security business requirements. As a result, we ended up with an overbaked set of documentation and leadership time commitment was higher than expected. These scars resulted in massive learnings that we could only get by implementing our own ISMS.

The real ugly part of the process was going through two failed attempts at our ISMS before setting up the implementation with a proper governance structure and dedicated resources. Regularly reporting our progress to the board kept us honest and on track.

When we got those things right, we nailed our ISMS implementation.

AHMED ELASHMAWY – Consulting Practice Lead and
TERRY CHAPMAN – Managing Director – *Axenic Ltd*

Visit https://www.axenic.co.nz/about/people/ to see more about Ahmed and Terry