MORRISEC
CLIENT CASE STUDY

TOUSTONE TRANSFORMS CYBERSECURITY STRATEGY WITH MORRISEC, ACHIEVING ISO/IEC 27001 CERTIFICATION

BACKGROUND

Toustone, a leading Australian data analytics company, recognising the need to strengthen its information security practices, embarked on a strategic initiative to enhance its security posture by pursuing ISO/IEC 27001 certification, a globally recognised standard for information security management.

We asked Toustone what the drivers were for getting ISO/IEC 27001:2022 certified:

> *"We had been toying with it for several years, but as the global incidents began clocking up, it became more pressing, and we recognised we needed the right partner to see us through to certification. We felt we already did information security well from a technical point of view, and when we were small, the lack of an information framework to support our measures was manageable. But as we grew, this became harder. The growth of Toustone also coincided with the rise in cybercrime, so the timing was perfect. Our clients needed more than our say-so that we did security well, and as it turned out, Morrisec was able to support us to do it better, as well as help us to develop the robust policies and framework needed to support certification."*

When starting their journey towards ISO/IEC 27001 certification, Toustone had only basic security policies in place, which needed to be significantly developed to meet the stringent requirements of ISO/IEC 27001. With the assistance of Morrisec, Toustone undertook a comprehensive program of work to build its Information Security Management System (ISMS) and achieve certification within nine months.

Toustone
Better data, smarter decisions.

INDUSTRY
Data Analytics

WEBSITE
https://toustone.com.au

CERTIFICATION CHALLENGES

▷ ISO/IEC 27001 is comprehensive and complex. Organisations struggle to understand the intent behind requirements and implemement them effectively in their business context.

▷ Conducting thorough risk assessments and developing appropriate risk treatment plans requires specialised knowledge many organisations may lack.

▷ Implementing an ISMS requires significant time and effort, and organisations often find allocating the necessary resources while managing their daily operations challenging.

▷ Developing policies and procedures tailored to the specific needs and context of the organisation can be complex without the right expertise.

MORRISEC

Toustone
Better data, smarter decisions.

We asked Toustone why they chose Morrisec as their security partner.

"The price was competitive, yet it also offered so much more, such as dedication and partnership, rather than just a project and a schedule of tasks to be completed. Recognising the importance of ongoing support after certification upfront and incorporating it into the proposal meant we had a plan to achieve certification and ensure longevity and that the effort wouldn't be in vain."

PROGRAM OF WORK

The program of work was divided into five stages, each focusing on different aspects of the ISMS development and implementation process. As Morrisec's Co-CEO, Dr Sarah Morrison, writes,

"By breaking the implementation process into five distinct stages, we can ensure an organisation is embedding the policies and processes being developed as part of the program of work and not just ticking a box. What is the point of implementing 27001, if not to improve your organisation's information security posture?"

STAGE 1: RISK MANAGEMENT

Morrisec began with a thorough organisational risk assessment to identify potential threats and vulnerabilities across the business. From this assessment, a risk register was developed along with the development of a Statement of Applicability (SOA), a requirement for certification based on the identified risks. A comprehensive information security risk framework was also established to effectively manage identified risks. Additionally, an asset register was created, and Morrisec commenced risk assessments across critical cloud providers being leveraged by Toustone as part of their business operations.

CERTIFICATION CHALLENGES

▷ Implementing technical controls to mitigate identified risks within your business operations can be complex, especially if the organisation lacks in-house security expertise.

▷ ISO/IEC 27001 requires continuous monitoring and improvement of the ISMS. Organisations often struggle to maintain the necessary vigilance and commitment over time.

▷ Conducting regular internal audits and reviews to ensure ongoing compliance can be resource-intensive and challenging without experienced personnel.

STAGES 2 & 3: ORGANISATION, PEOPLE & TECHNOLOGY CONTROLS

The second and third stages of Toustone's journey were to build out their information security framework, with the development of ISO/IEC 27001 required policies and procedures. As each policy was finalised and approved, Morrisec worked with Toustone to embed these policies and procedures into the organisation. For example, a security awareness calendar was created, and content was disseminated to educate Toustone staff on ISO/IEC 27001 requirements, general security awareness, and cyber-hygiene. The Morrisec team undertook third-party risk assessments across documented information assets, and any identified risks were captured in the risk register, with treatment plans documented. An Information Security Steering Committee was also established, and critical members of Toustone were appointed to oversee the work. Katie Scholten, Toustone's Privacy and Contracts Manager, describes her experience working with Morrisec during these project stages.

> *"One of the things we were impressed with regarding Morrisec's work is their availability. Morrisec was always there to back us up, no matter how ridiculous the question might be. Morrisec was one of the team."*

STAGES 4 & 5: ISMS CHARTER & AUDITS

Stages four and five were committed to auditing and ensuring Toustone was ready for their ISO/IEC 27001 internal and external audits. When the internal audit was due to commence, an independent auditor from Morrisec conducted and undertook the work as part of the service in preparation for the external audit. Throughout the external audit, Morrisec was the primary contact for the auditors, working as Toustone's CISO and managing all aspects of the stage 1 and 2 audits. Morrisec and Toustone's combined efforts successfully achieved ISO/IEC 27001 certification.

> *"Morrisec's preparation for the audit was amazing. We went into what could have been very stressful, reassured, and confident, as our consultant was very prepared and made sure we knew what to expect and were also prepared."* - *Katie Scholten, Privacy & Contracts Manager, Toustone*

CERTIFICATION RESULTS

- ▷ Improved identification, assessment, and management of information security risks, leading to a more secure organisational environment.
- ▷ Implement proactive security measures that prevent potential breaches and mitigate the impact of any security incidents.
- ▷ Meeting regulatory and legal requirements reduces the risk of fines and penalties associated with non-compliance.
- ▷ Streamlined and improved business processes through the implementation of well-defined policies and procedures.
- ▷ Assuring customers and stakeholders that their data is protected increases trust and confidence.
- ▷ Differentiating the organisation from competitors by demonstrating a solid commitment to information security.
- ▷ Establishing a culture of continuous improvement, where information security practices are regularly reviewed and enhanced.
- ▷ Increased employee awareness and understanding of information security practices lead to a more security-conscious workforce.

MORRISEC

POST CERTIFICATION SUPPORT

Since achieving certification, Morrisec has continued supporting Toustone in maintaining and enhancing its information security practices through various ongoing activities. This includes continually assessing and managing suppliers and third-party relationships, along with providing general security advice and guidance. Morrisec's ongoing security awareness training ensures continual growth of Toustone's cyber-aware culture and helps staff maintain vigilance against current and emerging threats. Incident response tabletop exercises are also conducted to ensure incident preparedness and timely response.

Additionally, Morrisec is responsible for the critical ongoing tasks required for Toustone to maintain its certification and ensure continual improvement. These include running monthly information security steering committee meetings and managing risk and asset registers to ensure they remain accurate and up to date. Morrisec also prepares and presents a six-monthly board report, including a detailed threat landscape analysis to ensure Toustone is aware of and can act against growing threats within its industry and geographical location.
Through these efforts, Morrisec has become an integral partner and part of Toustone's team, providing continuous support and guidance. As Katie Scholten from Toustone reflects,

> *"It is a big push to get ISO certification in place, but maintaining it is an even harder task. Other priorities and business issues arise, and we no longer have the bandwidth to dedicate to 27001. Having Morrisec onboard means we know we have it covered. Morrisec keeps us on track and makes the maintenance achievable."*

The collaboration between Toustone and Morrisec has resulted in a robust ISMS that not only achieved ISO/IEC 27001 certification but continues to evolve and improve. The structured approach and comprehensive support from Morrisec have ensured that Toustone maintains high information security standards, protecting its data and enhancing its overall security posture.

> *"What surprised us in our continued relationship with Morrisec is our consultant's willingness to give their time to adapt to our evolving needs and the flexibility our consultant and Morrisec's offer."*

MORRISEC

WHY CHOOSE MORRISEC?

Morrisec offers comprehensive ISO/IEC 27001 certification services to help organisations achieve and maintain their certification while enhancing their overall security posture. Unlike other providers offering generic, pre-written policies and procedures, Morrisec takes a tailored, risk-based approach to meet each client's needs.

Morrisec's unique methodology ensures that all documentation, policies, and procedures are customised to align with the client's existing processes, business requirements and future growth. This personalised approach not only aids in achieving certification but also ensures the effective implementation of an Information Security Management System that genuinely enhances security practices.

Morrisec is committed to achieving certification and ensuring its clients maintain and improve their security posture. By providing tailored solutions and ongoing support, Morrisec helps clients navigate the complexities of information security, making them a trusted partner in their security journey.

Toustone chose a three-year contract with Morrisec, dedicating the first year to achieving ISO/IEC 27001 certification. The subsequent two years are focused on maintaining the certification and acting as Toustone's security partner. This long-term commitment underscores Morrisec's dedication to its clients' ongoing security journey.

> "Toustone's relationship with Morrisec is very strong. Morrisec is part of the team. If you have any questions or issues, Morrisec is on hand to offer expert advice and practical support. We trust Morrisec's expertise and knowledge and know you have us covered for any cyber situation we face." *- Katie Scholten, Toustone.*

Post-certification, Morrisec remains an integral part of Toustone's team.

MORRISEC

MORRISEC - WHO WE ARE

Morrisec is a leading cybersecurity company that offers a broad range of specialised security solutions. Our services include governance, risk, and compliance (GRC); security awareness and digital supply chain defence; penetration testing; source code reviews and technical security consulting; secure development practices, including AppSec and DevSecOps; secure architecture design and review; and incident preparedness and cyber resilience. With a risk-based approach, Morrisec ensures that security controls are tailored to meet the unique needs of each organisation, securing and enabling business operations without disrupting critical functions.

In addition to our consulting services, we offer the Morrisec Risk Platform (MRP), a comprehensive tool that streamlines cybersecurity management. MRP delivers a unified, automated solution for managing assets, risks, and third-party suppliers, simplifying compliance and enhancing visibility. The platform supports Morrisec's ‘assess once, comply many’ approach, reducing the time, resources, and costs associated with compliance management. With real-time analytics and dynamic dashboards, MRP empowers organisations to make informed decisions and maintain a strong security posture, allowing them to focus on their strategic objectives and business growth.