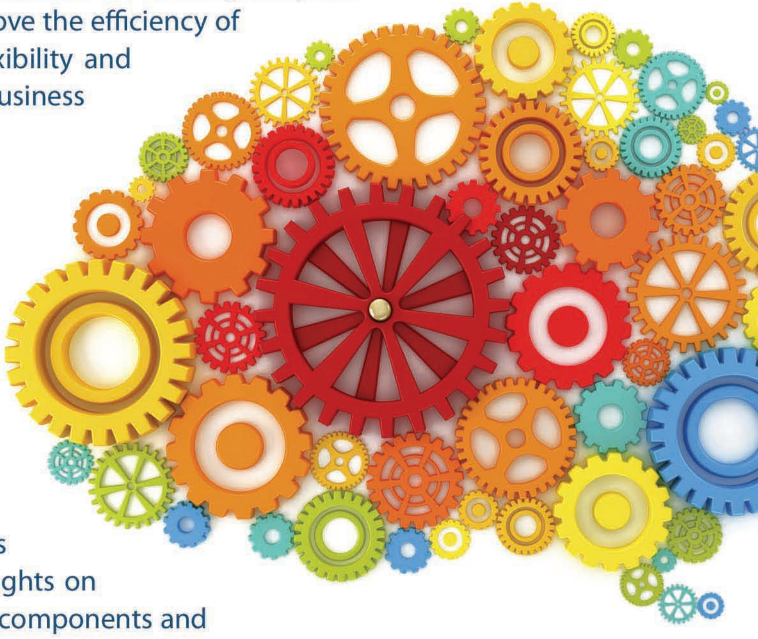
ISO 27001 CASE STUDY

verasseti
inquire, identify, improve

BACKGROUND

Verasseti (derived from the word veracity in line with the company ethos of truthfulness and exactitude) is a software development company which specialises in offering bespoke solutions designed to automate business processes and improve the efficiency of organisations. The company prides itself on having the flexibility and responsiveness of an SME, but the maturity and structured business processes associated with large corporate organisations.



In order to deliver its services, Verasseti requires access to sensitive and highly valuable data which is hosted on its own infrastructure. The company takes this responsibility very seriously and decided that achieving certification to ISO 27001, the International Standard for Information Security Management, was the most effective means of demonstrating its commitment to preserving the confidentiality of client data. Having started the certification journey in 2011, Verasseti achieved registration in 9 months and quickly realised a number of benefits. In this case study, James Percy, Director at Verasseti shares his thoughts on such factors as business drivers, project partners, key project components and benefits seen to date.

BUSINESS DRIVERS BEHIND DRIVE TO CERTIFY AGAINST ISO 27001

The decision to certify against ISO 27001 was both internally and externally driven. James Percy lists what he saw as the major ones.

- “ Having a corporate IT background, I appreciated the importance of providing multi-national corporates with the necessary reassurance that their data would be appropriately and adequately protected. We were also beginning to see ISO 27001 stipulated in contracts and tender responses.

- We believe ISO 27001 acts as a major differentiator between ourselves and other less mature software development organisations.

- I was well aware of the benefits to be derived from a structured and systematic approach to software development and data management from my corporate background. By certifying to ISO 27001, we believed that the management system would instil a greater discipline into the organisation’s culture as the Company grows and develops. ISO 27001 certification was, without question, not a box ticking exercise but a business enhancer! ”

SELECTION OF CONSULTANCY PARTNER

Whilst Verasseti was determined to own the development and implementation of its ISMS, James Percy acknowledged it could benefit from the guidance of an external consultancy organisation. Here James explains why Ultima Risk Management (URM) was chosen.

■ “It was clear that URM was very experienced in assisting organisations achieve ISO 27001 certification, but the critical factor in selecting URM was that they understood our business objectives i.e. understanding that this was not a box ticking exercise and the importance that the ISMS was fully embedded.

■ URM's 'lite' touch and focus on knowledge transfer was ideal in terms of our own need to be fully self sufficient. It also helped in ensuring systems and practices were appropriate to our culture and not over engineered. We were determined to understand every element of the certification process and URM's process enabled us to be involved in all stages and ensure all systems were fully embedded.

■ Another factor was URM's risk assessment tool (Abriska). Having a proven tool and methodology provided us with a lot of reassurance.”

SELECTION OF CERTIFICATION BODY

Verasseti had the choice of a number of certification bodies to act as the independent assessors of its ISMS. James Percy explains why British Standards Institution (BSI) was selected.

■ “For Verasseti, this was a simple decision due to BSI's association with quality and its credibility in marketplace. We felt that having a certificate signed by BSI definitely added to its value.

■ We were impressed by the approach taken by the BSI assessor. We found him constructive, approachable and diligent. Importantly, he was supportive of our desire not to over engineer solutions and to implement practical and appropriate working practices and systems ”

KEY STAGES OF THE CERTIFICATION PROCESS

James Percy identified the risk assessment phase as being key in developing its ISMS and in the ISO 27001 certification process.

■ “The risk assessment phase made Verasseti really appreciate the importance of managing risks and helped us identify and prioritise our risk treatment. The process allowed us to put the 133 controls of the Standard into perspective. It helped us understand what we were trying to protect, the risks we faced and how best we could draw on the controls to reduce our risks. Following the risk assessment, we introduced additional daily and weekly technical checks and revisited the levels of system access provided to both staff and associates. We also completely revamped our infrastructure and physical security.

■ The risk assessment highlighted a number of dependences on third parties and suppliers in particular. As a result, Verasseti now conducts audits on key suppliers and insists on new suppliers also holding ISO 27001 certification.”

At the centre of Verasseti's ISMS is the company's Information Security (IS) Policy. James Percy explains the significance of the Policy.

■ “The Policy sets out our approach to information security and why it is important to Verasseti. It also acts as the foundation of our staff awareness training programme. Through the IS Policy, we can clearly communicate to staff and associates their responsibilities in relation to maintaining the confidentiality of client information and our internal documentation.

■ Once associates have been provided with awareness training, they are asked to read and sign the IS Policy and are provided with reminders through ongoing awareness sessions. ”

BENEFITS SEEN

Verasseti started seeing benefits even during the actual process of achieving certification as James Percy explains.

■ “Externally, it was interesting to see how quickly we were perceived as a more attractive supplier and gained immediate tangible benefits in terms of winning new business. It has provided additional reassurances to existing customers, especially those who are already ISO 27001 certified and are aware of the processes involved. Having a certified information security management system (ISMS) definitely acts as a differentiator within our marketplace and has resulted in working practices and systems which are significantly more mature than our competitors.

■ Internally, I believe ISO 27001 has installed greater discipline and has led to improved working practices in areas such as back ups, access control, supplier auditing and HR controls. There is now a changed attitude to incident management, where the Company is far more confident in its ability to manage incidents as they occur. We try to learn from every incident in order to help minimise future recurrences.”

ADVICE TO OTHER ORGANISATIONS SEEKING ISO 27001 CERTIFICATION

James Percy concludes with his advice to organisations considering ISO 27001 certification.

■ “ The first thing to say is that it is not as onerous as one might expect. As ISO 27001 is risk based, it is not prescriptive and allows you to customise policies and processes and avoid over engineered solutions.

■ Do not look for perfection immediately. It is essential to build your ISMS over a period of time. As a software development company we already had a number of effective controls in place such as change control. However, the risk assessment helped us prioritise actions on some of the higher risk areas such as back up processes and supplier auditing.

■ It is important to view the process as one of continuous improvement, for example providing staff and associates with ongoing information security awareness training. With our software development skills, we have introduced automated reminders to ensure that different working practices are reviewed at regular intervals and any changes are fully communicated.

■ The selection of your consultancy and certification body partners is key. Ensure you find oganisations which are not only experienced but whose approach is compatible with your business objectives. Consultancy support can save a lot of time and effort and help you avoid going off at tangents. It is important at the outset to understand the complete process and roadmap and I would recommend you ask your consultancy partner to provide this. ”

For more information on URM’s ISO 27001 consultancy services:
Phone: 0118 9027 450
Email: info@ultimariskmanagement.com
www.ultimariskmanagement.com

For more information on Verasseti’s software development services:
Phone: 0845 1211 680
Email: inquire@verasseti.com
www.verasseti.com