ISO 27001 CASE STUDY

BACKGROUND

In April 2008 Marston Group, market leaders in high court and civil enforcement, gained certification to ISO 27001 the international Standard for information security management systems (ISMS). This case study highlights some of the business drivers, benefits derived and critical project success criteria. It also focuses on the roles played by the consultancy and training organisation Ultima Risk Management (URM) and certification body British Standards Institution (BSI).

In April 2008 Drakes Group Ltd, market leader in enforcement of warrants and liability orders and John Marston & Co, enforcement of high court writs, combined to become the leading provider of enforcement services throughout England and Wales. The Group, with 71 years experience in enforcement services, receives in excess of 800,000 warrants, liability orders and writs each year and is the dominant supplier to Her Majesty's Court Services (HMCS), Her Majesty's Revenue & Customs (HMRC), Child

DRAMATIC GROWTH OF GROUP

Following a management buy out in 2002, the Drakes element of the Group employed just 20 office staff and 40 bailiffs. Following the merger in April 2008, the combined Group employed 200 office staff and over 340 enforcement officers operating from a head office in Waltham Abbey, with regional offices in Waltham Abbey (separate from HO), Walsall, Sale, Billingham and Hove.

IMPORTANCE OF INFORMATION SECURITY

As one would imagine within this market sector, integrity and confidentiality of information (particularly personal data) is of the utmost importance. "Information is critical to the operation of a company and its survival" says Julian Thrussell, Standard Specialist at Ultima Risk Management. "Lapses in security have a serious impact on the credibility and brand of an organisation.

Although recovery may be prompt - memories last longer. Information and its protection is taken for granted and many organisations leave themselves open to its abuse, however Marston Group was able to recognise the importance of assessing its risks and to put in place suitable controls to limit any potential breaches." What was also important to the Marston Board was the ability to demonstrate to its government clients that the management system surrounding its information security was independently assessed and this was a prime driver for seeking ISO 27001 certification by a UKAS accredited organisation.

INCREASING PROFILE OF ISO 27001

Marston Group was aware that ISO 27001 was being increasingly referred to in public sector tenders and that a practical benefit of gaining certification would be a significant timesaving when completing pre qualification questionnaires (PQQs) and tenders. Achieving a 'meaningful' organisation-wide certification would also serve as a key benchmark within its sector and serve as a major differentiator in the demonstrable working practices adopted by itself and its competitors.

NEED FOR CONTINUOUS IMPROVEMENT

Frank Millerick, Chief Executive of Marston Group and the rest of the Board saw ISO 27001 being 'perfectly complimentary and central to the Group's commitment to continually improving the way we do business'. With this in mind in May 2007 the Board committed to seek ISO 27001 certification for all its offices. Within a year, Marston Group achieved its goal.

KEY ACTIVITIES

SETTING THE SCOPE

When deciding to certify, the Group made a conscious decision that this was not going to be a 'box-ticking' exercise, but one that would add real value. Marston was aware that by limiting the scope to one office or a particular function, time and money could be saved. However, the commitment from senior management was to include all offices and not just one within the scope of certification. The reasoning was that having a 'whole organisation' scope would provide the greatest reassurance to its government clients and provide added insurance should group certification be a prerequisite on future generation tenders.

BIA AND RISK ASSESSMENT

The business impact analysis (BIA) and risk assessment phases were led by URM with Russ Poulter, Audit and Compliance Director and Brian Heaven, Head of IT Support, shadowing all interviews. Russ found the process invaluable on a number of counts. "Whilst the BIA and risk assessment phase highlighted areas of risk we were already aware of, it also identified areas that the company had not fully taken account of or that the directors were not fully aware of. URM's BIA and risk assessment highlighted a number of areas, including the potential impact of a loss of availability of key information processing facilities and the need to achieve greater compliance with the Data Protection Act.

One of the impacts of the Group's dramatic growth between 2002 and 2008 was that parts of the IT infrastructure had not kept pace with the requirements of the organisation. These gaps, along with some of the resulting single points of failure, were identified in the risk assessment phase.

RISK TREATMENT PHASES

As part of the risk assessment phase URM used its automated risk assessment tool Abriska.

One of the outputs from the risk assessment was a report with a red amber green (RAG) diagram indicating the major risks to Marston. Russ Poulter and Brian Heaven found this report an invaluable starting point for risk prioritisation.

A major finding from URM's risk assessment was the need to implement new security related policies and processes throughout all areas of the organisation. This is where URM and Marston dovetailed neatly, with Russ Poulter working closely with the URM consultant to tailor URM template documents so that they were organic and met the cultural and working practices of the organisation.

Following the risk assessment, a number of new working practices were implemented including the introduction of clear desks for confidential information, improved password management, shredding of confidential information and locking down of PCs. Russ Poulter and Brian Heaven used a combination of tools and tactics to drive the culture change. Regular memos were sent to all staff detailing the changes being made and to act as reference points e.g. actions required to comply with the Data Protection Act (DPA).

A key component of the risk remediation phase was the security awareness training programme which was developed in conjunction with URM and then rolled out throughout the whole organisation, including remote workers (enforcement officers), using newly appointed local security coordinators (LSCs) at each location. A focus of the training was to personalise the messages and to encourage staff to treat personal data they were processing as though it belonged to a member of their family. Built into the training was a multi-choice answer quiz which served not only as a guide to assess the effectiveness of the training, but as a benchmark for future measurement and comparison.

CRITICAL SUCCESS CRITERIA

SENIOR MANAGEMENT COMMITMENT

At all stages of the ISO 27001 certification project, senior management not only endorsed and supported new policies and procedures, but also 'led from the front'. Typical of this was that it was directors who were the first to adopt new working practices. This again leads back to the fact that a driver for adopting ISO 27001 was the need to 'improve the way we do business' and not just an exercise to gain a new badge.

FRESH START

Russ Poulter, with the assistance and commitment of the IT department, used the Christmas/New Year break as the ideal time to introduce a 'fresh start' as far as implementing new policies and procedures e.g. locking down PCs and improving password controls. The company used this period to introduce a number of physical changes e.g. introducing new software, changing screen savers and locking down unused ports. These highly visible changes to the environment were very effective in serving to reinforce the new working practice regime.

COMPREHENSIVE MONITORING AND AUDITING PROGRAMME

As an organisation that was already certified to ISO 9001 by a UKAS accredited organisation, Marston was already converted to the merits of following the plan-do-check-act model of continuous improvement. The importance of continuous auditing and monitoring was already fully embraced and Marston has developed a sophisticated three tier model for ensuring compliance of enforcement officers (remote workers), as well as office staff. Marston also fully utilized LSCs and line managers to encourage adoption and monitor new security measures. Monitoring activities included spot checks to ensure that, for example, PCs had been locked down when users were away from their desks or that confidential information was not left lying on desks at the end of the working day. Users often returned to their desks to find sticky notes with either a smiley or frowning face!

COMMUNICATING BENEFITS TO ISO 27001

When developing the security awareness training programme every effort was made to make the messages as accessible and relevant to all staff. Asking call centre staff to view and treat information as though it belonged to a family member was one method. Another approach was to stress the benefits that the whole organisation would derive from improved security, including greater job security and personal development.

INTEGRATING ISO 27001 INTO DAY TO DAY BUSINESS ACTIVITIES

Marston always took great care to ensure that ISO 27001 was not seen as a discrete and separate activity, but something that was fully integrated into 'business as normal' and thus policies and procedures were developed in such a way to ensure maximum possible adoption.

SELECTING KEY PARTNERS

ULTIMA RISK MANAGEMENT (URM)

The selection of URM, a consultancy and training organisation experienced in assisting organisations achieve ISO 27001 certification, was a key one and led to a number of benefits including:

- Gaining an independent and fresh perspective, particularly at the risk assessment stage and where it is often easier for an external consultant to ask the difficult and challenging questions
- Finding a consultancy which not only provided advice, but played an active role as part of the team in the implementation of policies and procedures
- Introducing a proven risk assessment tool with management reports which helped to prioritise risk treatment activities
- Working with a consultancy which was keen to transfer as much knowledge as possible and promote self sufficiency
- Introducing policies and procedures templates which could be adapted to meet Marston's culture and requirements.

BRITISH STANDARDS INSTITUTION (BSI)

When considering which certification body to engage in its certification process, there was little doubt in the mind of Marston which certification body to choose. British Standards Institution (BSI) satisfied all of the following key requirements:

- A certification body which was United Kingdom Accreditation Services (UKAS) accredited
- A globally recognised brand that would enhance the status of the certification due to its reputation for integrity and rigour when assessing
- The involvement of the Standard Division of BSI in the development of ISO 27001
- The experience of being involved in certifying more ISO 27001 ISMS' than any other certification body, BSI was in the best position to providing insightful and pragmatic advice over implementation
- As a market leader in ISO 9001 certifications, BSI was ideally positioned to assess both management systems.

BENEFITS SEEN

IMPROVED SECURITY

\One of the major reasons behind the decision to certify against ISO 27001 was, quite simply, the desire to continually improve the way the organisation did business. Even by the time Marston was going through its Stage 1 and Stage 2 assessment, it was acknowledged within the senior management team that significant and tangible improvements had already taken place. A number of the weaknesses and single points of failure identified in the risk assessment phase had been addressed by the time of certification. Whilst security is naturally difficult to objectively assess, Marston believed that controls implemented as part of the certification process have helped to reduce the possibility of security breaches taking place.
At the same time the Group is well aware that iso 27001is a journey of continuous improvement and that ongoing vigilance and awareness are key.

IMPROVED TRUST AND REASSURANCE

At a time when a series of high profile information security breaches involving various government departments and large financial institutions were occuring, it was essential for Marston to provide its existing government clients with the maximum confidence that information security within the Group was being given full attention.

ISO 27001 certification also served to provide new clients with reassurances that the Group can be trusted in the processing of any personal data. Marston has been keen to stress to clients the full scope of the certification i.e. all offices included and not just a subset and the fact that the certification process had been conducted by the most experienced and recognised CB i.e. BSI.

REDUCTION IN TIME TO COMPLETE TENDERS

A very practical benefit derived from gaining certification has been a reduction in the time and resources needed to complete public sector tenders and pre qualification questionnaires (PQQs). Achieving certification has negated the need to complete substantial elements of the tenders or questionnaires.

PART OF PROFESSIONAL DEVELOPMENT

The professional development of all staff is a key business goal at Marston and the ongoing information security awareness training being provided to office and remote workers is seen as a central to personnel development.

SUMMARY

"During the implementation of ISO 27001, Marston Group's information was considered with confidentiality, availability and integrity in mind. Successfully managing this delicate balance proved to be a very worthwhile exercise, highlighting clear improvements in working practices and critically, customer interaction," says Julian Thrussell, Standards Specialists at URM.

"Throughout the project there has been continued senior management commitment to the project which underpins the importance of the certification to the business as a whole. Certification to ISO 27001 has enabled continual monitoring and improvement of Information Security performance by regular assessment programmes. Marston's can be rightly proud of their commitment to both their customers and their business."

As Lisa Dargan, Business Development Director at URM adds " This was never going to be a tick in the box exercise for Marston Group. Right from the start certification to ISO 27001 was seen as a way of improving the way the Group does business and this goes a long way to explaining why the new Information Security Management System was implemented so successfully".

URM
ULTIMA RISK MANAGEMENT

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

bsi.

For more information on certification to ISO 27001 with BSI:
Phone: 0845 080 9000
www.bsigroup.co.uk/infosec