



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 Information Security Management System (ISMS) Standard. This case study highlights some of the business drivers, benefits derived and critical project success criteria.

Marston Group was created in 2008 when Drakes Group Ltd, market leader in enforcement of warrants and liability orders combined with John Marston & Co, enforcement of High Court writs 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 Support Agency (CSA) and High Court markets.

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. After the merger in April 2008, the combined Group employed 200 office staff and over 340 enforcement officers operating from a head office (HO) 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, Product Marketing Manager for BSI Management Systems UK. "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."

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 United Kingdom Accreditation Services (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 and major differentiator within its market sector.

Need for Continuous Improvement

Frank Millerick, Chief Executive of Marston Group and the rest of the Board saw ISO 27001 being "perfectly complementary 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. There was also a genuine desire to improve policies and processes across the Group in line with its quality objectives and for staff in all areas to develop greater security awareness.

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. This is where you can really benefit from a fresh and objective perspective from an external organisation like Ultima Risk Management." 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 27001. 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 clearing desks of 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. This 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.

Monitoring and Auditing

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 developed a sophisticated three tier model for ensuring compliance of enforcement officers (remote workers), as well as office staff.

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'. Typically, it was the directors who were the first to adopt new working practices. This again reinforces the fact that the driver for Marston's adoption of 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. The company used this period to introduce a number of physical changes e.g. introducing new software, changing screen savers, improving password controls and locking down unused ports. These highly visible changes to the environment were very effective in serving to reinforce the new working practice regime.

Utilising Local Management in Monitoring and Auditing

In order to ensure information security was fully embedded into the organisation, Marston fully utilised

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 'post-it' 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 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'. 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 ISO 27001 certification, led to a number of benefits including:

- Gaining an independent and fresh perspective, particularly at the risk assessment stage
- 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
- Introducing policy and procedural templates which could be adapted to meet Marston's culture.

BSI Management Systems

When considering which certification body (CB) to engage in its certification process, Marston had little doubt which one to choose. BSI Management Systems satisfied the following key requirements:

- A CB which was UKAS accredited
- A globally recognised brand
- The reputation of the Management Systems Division for its integrity and rigour when assessing
- Having been involved in certifying more ISO 27001 Information Security Management Systems than any other CB, BSI was in the best position to provide insightful and pragmatic advice
- As a market leader in ISO 9001 certifications, BSI was ideally positioned to advise on integrating the two 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. 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 it had implemented controls which had helped and would help to reduce the risk of any security breaches taking place.

At the same time the Group was well aware that this was a journey of continuous improvement and that ongoing vigilance and awareness would be essential.

Improved Trust and Reassurance

At a time when there have been a series of high profile information security breaches involving various government departments and large financial institutions, 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 reassurance to new clients that the Group could be trusted in the processing of any personal data. Marston was also 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 certification body i.e. BSI.

Reduction in Time to Complete Tenders

A very practical benefit that has been derived from gaining certification is a reduction in the time and resources needed to complete public sector tenders and pre qualification questionnaires (PQQs). Achieving certification typically negates 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 information security awareness training being provided to office and remote workers on an ongoing basis 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, providing customers with additional reassurance,” says Julian Thrussell of BSI Management Systems UK

“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 can be rightly proud of their commitment to both their customers and their business.”

As Lisa Dargan Business Development Director of URM adds “ This was never going to be just 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 has been so successfully implemented.

For further information please contact Ultima Risk Management Ltd

Tel: 0118 902 7453 Email: info@ultimariskmanagement.com Web: www.ultimariskmanagement.com