



ISO 27001 Case Study

systems + services UK Ltd

Background

a&o systems + services UK Ltd is a leading provider of IT infrastructure services & systems support with a head office located at Colnbrook in Berkshire, close to Heathrow Airport. The company offers a comprehensive portfolio of services aligned across three broad areas 'Enterprise Services & Solutions', 'IT Service Management' and 'IT Service Support'. a&o's services are typically adopted by medium or large enterprises, public sector organisations, IT outsourcers, service providers or original equipment vendors. The Colnbrook office is a 24 x 7 operation housing both a Managed Services offering (Service Desk) for direct customers and a Call Centre for indirect customers.

Underpinning a&o's market offerings is a total commitment to providing consistently high quality and environmentally friendly services. This commitment is clearly demonstrated by the Company's adoption of globally recognised management system Standards such as ISO 9001 (quality management system) ISO 14001 (environment management) and PAS 99 (specification of common management system).

Seeking certification to ISO 27001, the international Standard for information security, was a natural progression for a&o. Paul Smith Quality Manager at a&o explains "We were mindful of the fact that ISO 27001 was, and increasingly continues to be, referred to in a number of public sector tenders. When it became a mandatory requirement in a specific Service Desk health sector related tender, it became a straight forward decision. As well as having the natural blessing of the Sales Director, the decision to certify was supported by all the senior management team including the Client Services Director and Managing Director."

In May 2007, a&o embarked on a project to certify information security management system (ISMS) against ISO 27001. Within just 7 months a&o had achieved certification. This case study looks at the process that a&o followed in achieving certification, how the Company managed to achieve it in such a short timescale and what benefits it has seen as a result.

Key Stages in a&to's ISO 27001 Project

1 Selecting Partners

Whilst a&to was familiar and confident with the operations of a management system, it felt it could benefit from working with an ISO 27001 specialist consultancy. a&to chose to work with Ultima Risk Management Ltd (URM). What impressed a&to was the clarity URM brought to the process, its robust and proven risk assessment methodology and the strong knowledge transfer ethos.

The other decision was the selection of a certification body (CB) and the natural choice for a&to was British Standards Institution (BSI) the market leading CB for ISO 27001 and the organisation which a&to had selected to assess its other management systems. At the pre assessment visit a&to felt reassured by the BSI Assessor's constructive and precise feedback.

2 Setting the Scope

The scope of the proposed certification was confined to the Service Desk. "It was a conscious decision" comments Paul Smith "to achieve certification with a restricted scope against a tight timescale, learn from the process and then consider extending the scope in the future to ultimately encompass the entire UK organisation."

3 Risk Assessment (Plan Phase)

This stage of the project is where a&to leant heavily on the expertise of URM and in particular URM's risk assessment software. URM conducted interviews with all a&to's senior managers to assess what the impact would be of a breach of information security. Following the business impact analysis (BIA), key managers were interviewed in order to assess what threats could lead to such an impact both from a likelihood and vulnerability perspective. With all the key data being inputted into URM's risk assessment tool the end product was a risk assessment report which prioritised a&to's major threats into red, amber and green using a RAG diagram.

4 Risk Treatment (Do Phase)

Having identified the key risks, the next stage involved deciding how to deal with these risks. "Whilst there were no major surprises" comments Brian Wathen, a&to's Client Services Director "the RAG diagram produced at the risk assessment stage was invaluable in helping prioritise our remediation work. What the risk assessment highlighted was that whilst we had been adopting good practice in a number of areas there was a lack of formality and documentation surrounding some of the working practices. A good example was the lack of central logging of potential security incidents. Contracts and agreements with suppliers were also reviewed to ensure that suppliers too were adopting good information security practice."

5 Developing and Integrating Management Systems (Do Phase)

With its previous investment in ISO 9001, ISO 14001 and PAS 99, a&to was keen not to reinvent any wheels and use existing structures as much as possible. Developing its security policies and processes as part of its information security management system (ISMS), a&to went to great lengths to ensure that it integrated ISO 27001 as effectively as possible with its ISO 9001 management system.

As Andrew Morris, Business Development Director of BSI UK Management Systems observes "We are seeing an increasing trend towards the integration of Management Systems such as ISO 27001, ISO 9001 and ISO 14001. The benefit of doing so is the development of a holistic corporate business wide management system which is far more likely to be embedded into the culture of the organisation. By integrating different management systems and avoiding a silo approach, organisations can maximise existing investments by reusing common components and avoid duplicating procedures."

6 Reviewing, Auditing and Improving (Check and Act Phases)

With its understanding of other management systems and the concept of continuous improvement, a&to felt increasingly confident to take the lead role in the later life cycle phases and use URM more as a 'sounding board'. With extensive experience of internal audit and review processes, a&to quickly became self sufficient with URM adding guidance and advice as and when required.

7 Assessment Visits from BSI

In order to gain ISO 27001 certification an organisation must go through a two stage audit process with an accredited certification body. a&to chose BSI Management Systems, the world's leading for information security and the UK's best known. Stage 1 is a document review where the auditor reviews the ISMS e.g. scope, policy, risk assessment process, statement of applicability. Stage 2 is an objective assessment of the organisational procedures and practice carried out against the documented ISMS which was reviewed in Stage 1. Stage 2 involves staff interviews, both with those responsible for managing the security environment and those working in it. a&to encountered no issues at either stage, due in main to its meticulous preparation, the risk assessment process and project guidance from URM as well as the precise feedback from the BSI pre assessment audit.

Key Project Success Criteria

Paul Smith, Quality Manager at a&to, was quick to identify some of the key factors behind what was seen widely as a very successful project:

Senior Management Commitment

This was undoubtedly one of the major success factors with senior management, not just supporting the project, but actively participating and embracing it. Indicative of this is that security quickly became a fixed item on the senior management meeting agenda. ISO 27001 became not just a box ticking exercise but something that was perceived as having real tangible business benefits.

Internal Champion

a&to had not one but two champions, namely himself as the Quality Manager and Guch Bhamra the Managed Services Manager. Both ensured that momentum was always maintained and that the project kept to its tight deadlines.

Limited Scope and Challenging Timescale

By limiting the scope to a key part of the business (the Service Desk) the remediation phase became more manageable and achievable within what was an ambitious timescale. Although the timescale for certification was challenging, one of the major counter benefits was that the project never lost impetus.

Familiarity with Management Systems

Having experience of implementing and maintaining other Standards, such as ISO 9001, helped the process and a&to was able to reuse existing management systems which negated the need to introduce staff to new systems and working practices.

Security Awareness Sessions

a&to went to extensive lengths to provide all staff concerned not just with training on ISO 27001 controls, but on the reasons why the Standard was being adopted and how the Company and they would personally benefit. Formal training was followed up by ad hoc spot checks to ensure key messages, such as locking down PCs, became ingrained into working practices.

Dovetailing with Partners

A primary goal for a&to with this project was to find a consultancy partner who would be flexible in its approach. What a&to found with URM was a consultancy company that was happy to provide skills and transfer knowledge in areas where there were gaps, notably with its practical and proven risk assessment methodology. But equally a&to found a consultancy that was happy to take a back seat as the project progressed with a&to taking control of the implementation and ownership of the management system

ISO 27001 became not just a box ticking exercise but something that was perceived as having real tangible business benefits.

Benefits Gained

Objective Assessment of Risks

Like many organisations a&to believed it had a good intuitive feel for its information security risks. What URM's risk assessment (including BIA) provided though was a structured, formalised and consensus approach, which not just documented the major risks, but assisted a&to in prioritising its risk treatment activities.

Operational Improvements

Having identified the major threats to the organisation, a&to was able to immediately implement a number of quick win controls including central logging of security incidents, clear desk working, locking down of PCs and improved disposal of physical documents. Paul Smith believes that the 'demand for greater discipline' is one of the major benefits that Standards such as ISO 27001 brings to any organisation.

Security Embedded in the Culture

Interestingly, the benefits of certifying to ISO 27001 were not limited to just the original scope i.e. Service Desk area. Paul Smith observed that "despite some initial scepticism from certain departments, there has been a ripple effect throughout a&to. The use of cross shredders to dispose of confidential paper records has spread though other departments as has the adoption of security enabled Xerox printers. The classification of information is also being rolled out throughout the whole organisation."

Any visitor to a&to's Service Desk area in Colnbrook can not fail to be impressed by an organisation which has fully embraced information security. Working in a secure area, all desks are completely free of any paper records and all vacant desks are locked down. Following certification to ISO 27001, Guch Bhamra has also observed a real sense of pride and achievement within his team. On the walls of the Service Desk room is not just a copy of the ISO 27001 certificate, but also a copy of the Company's information security policy.

Commercial Benefits

The initial tipping point for gaining ISO 27001 certification was to meet the requirements of a particular customer which was involved in a National Health Service (NHS) Contract. Paul Smith believes ISO 27001 has "already opened a number of doors for our Service Desk as far as public sector tenders are concerned and certainly helps in any short listing process. For those potential customers who need tangible evidence of a supplier's commitment to information security, there is nothing to compare with ISO 27001. In a similar way, we are now looking for similar reassurances from our suppliers."

What URM's risk assessment (including BIA) provided though was a structured, formalised and consensus approach, which not just documented the major risks, but assisted a&to in prioritising its risk treatment activities.

For further information please contact Ultima Risk Management Ltd

Tel: 0845 838 2084 Email: info@ultimariskmanagement.com Web: www.ultimariskmanagement.com