Dual ISO 27001 and BS 25999 Certification

Case Study

Background

In the UK automotive industry, Audatex (UK) Ltd is the undisputed market leading provider of computerised estimating and claims management solutions. The company works in partnership with leading insurance organisations, bodyshops, motor manufacturers and all parties involved in the supply chain to provide solutions that ensure speedy and effective resolution of insurance claims. Based in Theale, Berkshire, Audatex is part of the Solera group of companies, a global provider of claims solutions. Solera's operating companies employ over 2,000 associates in over 50 countries across 6 continents, and have a global network of over 50,000 customers.

As a leading edge technology company and innovative market leader providing a critical and pivotal role within the claims supply chain, Audatex has been acutely aware of the need to provide its partners with the confidence that it is doing everything within its powers to guarantee both service delivery and the security of any shared data. As a consequence, Audatex has proactively invested considerable resources in its IT infrastructure and in its service continuity capabilities. At the same time, the company has also acknowledged that technology can only provide part of the total solution, just as important are the people and working practices.

The challenge for Audatex was to decide on the best ways of developing robust internal systems and strong management practices in both information security and business continuity. Attainment of the respective management standards, ISO 27001 and BS 25999-2 was seen as an ideal way to demonstrate this.

Ross McEleny, IT Services Director, Audatex UK became aware of the advantages of both of these standards and quickly saw the value that Audatex could derive from dual certification following discussions with British Standards Institution (BSI). This opinion was shared by Paul Tucker, Managing Director, Audatex UK, as well as other members of the senior management team.

As Ross McEleny explains; the major difficulty was choosing which Standard to adopt first. "There were strong business drivers for certifying to both and we were really keen to demonstrate to all our stakeholders our proactive approach in the adoption of best practice both in terms of business continuity and information security. Following a number of internal and external discussions on which to address first, we made the bold decision to become the first global organisation to simultaneously certify to both"

This case study focuses on the process which Audatex, with the assistance and guidance of consultancy partner URM, went through in becoming the first organisation to achieve simultaneous certification to BS 25999 and ISO 27001, along with an assessment of the critical success criteria and benefits gained.

Key Stages in Achieving Dual Certification

Setting the Scope

Having committed to certifying to both standards, the next decision for Audatex was setting the scope of the certifications. As Paula Robinson, Information Security Manager and the appointed BS 25999 / ISO 27001 project champion at Audatex explains "Focussing on just one area would have led to the need to set up service level agreements between different areas and the creation of artificial internal boundaries. At Audatex, everything is so interlinked we concluded that the most realistic and meaningful scope was to certify the whole operation at Theale. This, naturally, would also provide all our stakeholders with the greatest value and reassurances."

Risk Assessment Phases

It was during these early phases that Audatex leant heavily on the expertise of URM. As Lisa Dargan, Business Development Director of URM explains, the risk assessment phases for BS 25999 and ISO 27001 were two distinct and different exercises. "Throughout the project we were looking to combine activities and minimise management time. Whilst it was possible to achieve this in later stages, this was not feasible with the business impact analyses and risk assessments. In essence with BS 25999, senior management is being asked how long it believes the business can survive without certain critical activities and with ISO 27001 it is having to assess the impact of a security breach (involving either a loss of confidentiality, integrity or availability). Having assessed business impacts one is then assessing the risks which could lead to these impacts and risks which could hamper the recovery process." As Paula Robinson takes up this theme, Audatex found this exercise invaluable. "There were no real surprises with either of the two risk assessments but both provided a collective perspective which allowed us to prioritise our risk treatment.

Training and Communication

Paula Robinson identified the security awareness sessions alongside the introduction of access cards as being of pivotal importance in obtaining buy in from staff to the cultural changes, such as clear working environments and locked down screens. Understanding the benefits to the organisation and ultimately to themselves helped with the phasing in of new policies and procedures.

Risk Treatment Phases

As the project moved from risk assessment to risk treatment, so Audatex began to take greater ownership with URM's consultants providing more of an advisory role. The emphasis was placed on increasing the levels of integration between the two certification strands. As Paula Robinson observed "Whilst availability was the initial focus, the risk assessment highlighted any loss of confidentiality and integrity were also equally critical to the organisation. Thus there was a degree of overlap between the controls required to treat both ISO 27001 and BS 25999 risks." One of the key issues identified from both risk assessments were single points of failure which has led to increased levels of procedural documentation and knowledge transfer activities. Access control both physically and logically was another area to be tightened following the risk assessment, which included the introduction of proximity access cards. "This overt physical change" comments Paula Robinson "represented a watershed as far as staff awareness was concerned and certainly helped raise the profile of the project in everybody's minds."

Integrated Management Systems

Whilst attempting to certify against two Standards presented some tough challenges, one benefit was the implementation of an integrated management system. The most effective management system is one which is regarded as simply 'the way the business works' and one based on continuous improvement or 'plan, do, check, act'. Within management system standards (including ISO 27001 and BS 25999), there are a number of common components and these include management reviews, corrective action, preventative action, control of documents, control of records, internal audits and formal documentation of policies, processes and procedures. Audatex was determined to avoid a 'silo' approach and duplication of effort and thus implemented an integrated business wide management system which would serve both BS 25999 and ISO 27001 standards.

Critical Success Criteria

Senior Management Commitment

“Without senior management commitment” comments Paula Robinson “the project quite simply would not have been successful. With a companywide scope and a holistic management system it is critical that there is cooperation from all parts of the organisation. Without the support of the Managing Director and other Directors which make up the Steering Group, staff would simply not have seen ISO 27001 and BS 25999 as priorities.” As it is, information security and business continuity feature strongly within the Company Meetings which are held twice a year and chaired by Paul Tucker, the Managing Director. The project also featured within the objectives that were set for all employees.

Internal Champion

As with all projects there has to be a dedicated internal driving force and in the case of Audatex this was Paula Robinson. Inevitably other business pressures are going to arise and there will be times when progress is slow. At these times, it is down to the tenacity of the project manager to maintain the momentum of the project.

Customisation and Integration

As part of the risk treatment phase, Audatex introduced a number of new policies and procedures. Whilst referring to URM for guidance on the essential components of policies and procedures, documents were edited in an Audatex house style to make them as accessible as possible. As Paula Robinson explains “We were determined to ensure that we integrated both certifcation projects as much as possible into our normal way of working.”

Awareness Training and Communication

As seen in many other certification projects a vital success criteria is staff awareness training and the utilisation of multiple communication channels. This is certainly one area where Audatex excelled. Every member of staff (be they permanent or temporary) has gone through a BS 25999/ISO 27001 awareness session and this session now forms an essential part of new starter’s induction process. In terms of communication channels Audatex has used a multipronged approach. Apart from the twice yearly Company meeting, monthly deparmental breakfast meetings are utilised to update staff on the progress of the project. In addition, internal web pages are used for posting key information or dates. Another vehicle that will be utilised is the Human Resource Information System/portal.

External Expertise

Audatex, whilst determined to shape, own and manage its management system acknowledged that it could benefit from external support in specific areas. URM was particularly valuable in bringing specific expertise to the party e.g. conducting risk assessments, testing business continuity plans and conducting internal audits. This also saved Audatex considerable time in learning from an expert. Another factor that greatly assisted the certifcation assessment process was that BSI was able to provide a single assessor who conducted both ISO 27001 and BS 25999 assessments. This was an important benefit taking into account the integrated management system.

Selecting Key Partners

Consultancy

Audatex invited a number of consultancies to submit proposals on how they believed they could best assist the company to achieve dual certification as well as presenting their credentials. The consultancy chosen was URM a company that specialises in providing training and consultancy services in the fields of both information security and business continuity. URM’s training pedigree and the knowledge transfer ethos espoused by URM was important to Audatex, as it was determined to find a partner it could both work with and learn from, rather than find a consultancy which would take over and just get the ‘tick in the box’.

Certification Body

Following its involvement in supporting PAS 125 the technical specification for the process of vehicle body repair, Audatex had already come into contact with BSI and was aware of BSI’s pre eminent position as the leading ISO 27001 certification body (CB) and even more so as one of the major driving forces behind the new BS 25999 Standard. The combination of an existing relationship and BSI’s leading certification brand made the choice of certification body very straight forward.

Benefits Seen

Improvements in Security and Reductions in Risk

Following the risk assessments a number of single points of failure were identified and the associated risks were addressed through more detailed documentation of procedures and knowledge transfer activities. Measures have also been taken to provide greater resilience around services and information provided by third parties. As a consequence of risk assessments new supplier guidelines have been implemented involving due diligence activities.

Staff Changes in Attitude

Following security awareness sessions, clear working environment and clear screen policies were implemented. One of the most encouraging and pleasing aspects has been the attitude to reporting of security incidents. There has been a discernible change in culture to a far more open 'no blame' environment where incidents are discussed and lessons learnt. The whole certification project has also led to a more integrated and holistic business processes e.g. the development of company-wide documentation policy.

Customer Confidence and Reassurance

Even before becoming certified, Audatex had observed an increasing awareness among its customers of the need and value of implementing best practise in information security and business continuity. The dual certification project was a clear statement of intent that Audatex fully appreciated the importance of keeping data secure and the importance attached to continuity of service delivery. By adopting the currently accepted best practice in both areas and having its management systems certified by a leading independent authority, has enabled Audatex to provide customers and stakeholders with the most effective form of reassurance.

Easier to Comply with Other External Requirements

During the implementation of the management standards, Audatex had an imposed requirement to implement a Sarbanes-Oxley control framework within the financial areas and is also adopting ITIL best practise within the IT department. Audatex recognised that by incorporating common elements from these different frameworks in to a wider integrated business management system transferable holistic benefits would be seen across the organisation.

Summary

Julian Thrussell, BSI's Product Manager for Risk Standards including BS 25999 and ISO 27001 comments on the dual certification "Audatex's early decision to combine the implementation of both standards, significantly reduced the time overheads involved. The ability of BSI to supply trained assessors to combine parts of the assessment was also beneficial. Senior management engagement and support added a real impetus and drive, which was visible to the assessor from the start. Every now and again a company stands out in its approach and success, Audatex can be justifiably proud."

"As a global provider of claims solutions we operate at the highest level in terms of information security and business continuity," says Paul Tucker, Managing Director, at Audatex. "Being the first company in the world to simultaneously attain both the ISO 27001 and BS 25999 management system standards is an important achievement; underpinning our continuous improvement strategy and demonstrating our ability to lead the way by adopting internationally recognised business standards. We were in good shape before we started working towards dual certification but the steps to achieving this focussed our attention on identifying and removing potential risks. URM's guidance throughout this process was invaluable."

For further information please contact URM
Tel: 0118 206 5410 Email: info@urmconsulting.com Web: www.urmconsulting.com