BACKGROUND

UK Mail is one of the largest express delivery companies in the UK, with 40 years of experience tailoring domestic and international mail and parcel delivery services for its customers. It also provides courier and other special logistics services.

UK Mail's services are provided through a network of over 3000 owner van drivers operating out of approximately 52 depots and mail sortation centres throughout the UK. UK Mail also owns and operates over 200 larger vehicles which transport bulk mail around the country between these centres and onto final mile delivery by Royal Mail.

A notable service offered by UK Mail is its imail solution which enables individual customers to create, print and deliver their mailings all through one, easy to use online application, providing them with greater convenience and significant cost savings over traditional design, print and mail services.

In July 2014, UK Mail achieved certification to ISO 27001:2013 (the International Standard for Information Security Management) with a scope that covered the entire UK business, excluding UK Pallets. This case study details the business drivers, key stages, success criteria and benefits derived that accompanied UK Mail's journey to ISO 27001 certification.

Business Drivers

There were a number of business drivers behind UK Mail's decision to certify to ISO 27001. One major factor was that UK Mail had experienced a significant increase in demand from its public and private sector customers for assurance of its information security management arrangements and capability. Certifying to an internationally recognised standard, such as ISO 27001, would serve not only to demonstrate compliance with good practice, but also to emphasise UK Mail's ongoing commitment to information security.

KEY STAGES

Selection of Key Partners

UK Mail's IT led implementation team, with its own business challenges, recognised that it could benefit from bringing on board a partner with proven ISO 27001 implementation and certification experience.

Tony Smollett, Group IT Director, comments "We operate in an ultimately pragmatic, next day environment and it was really important for us to find a consultancy partner who could work with us in such an environment. URM was selected because of its practical and flexible approach, along with its extensive ISO 27001 track record and experience."

Certification Europe was selected as the certification body due to the cultural fit with UK Mail, having been identified as an established brand looking to grow in the UK. It also produced a flexible proposal that maximised the audit schedule without compromising on full coverage of UK Mail's business.

Risk Assessment

UK Mail benefitted from using URM's expertise and its risk assessment tool, Abriska™, to conduct an initial information security risk assessment ahead of making any decisions on its certification scope. Collecting and consolidating a significant amount of information and enabling it to be interpreted quickly and easily, URM helped UK Mail to make strategic implementation and risk treatment decisions in the short timescale required.

Scope

In exploring certification scope options, UK Mail initially considered an IT based product related scope, along with a possible expansion to include its Birmingham location. However, before committing to an agreed scope, UK Mail followed URM's recommendation and conducted an information security risk assessment across all of its sites to better understand the business' risk profile. The results showed that operational risks could be managed through a small number of risk entities, rather than being managed as individual site entities; this made the possibility of certifying the whole of the business far more feasible.

Focusing on the business' needs to provide assurance to customers of its capability to protect information throughout its network, UK Mail sought to pursue the scope which offered the greatest value to its customer base. With this in mind, UK Mail decided to certify all its sites, irrespective of product, service line or location. Whilst the geographical scope across the UK was challenging, this implementation of information security controls was eased by UK Mail's various standardisation initiatives and its ability to centrally manage a significant proportion of its controls, thereby maximising its return on investment.

Planning and Developing the ISMS Infrastructure

Documenting UK Mail's information security management system (ISMS) framework was a key initial activity in the certification project and proved invaluable in helping to articulate, internally and externally, how the management system operates. Capturing its context, stakeholder considerations, governance arrangements and key management system processes, URM offered guidance on formalising and integrating management system activities. One key objective of implementing the ISMS was to maximise the use of existing business processes and procedures by utilising and adapting them in the most pragmatic manner.

Prior to embarking on its ISO 27001 certification project, UK Mail had already developed a suite of information security policies. URM's consultants worked with UK Mail to make the policies more accessible to the whole organisation by rationalising these and ensuring that they meet the requirements of the revised ISO 27001:2013 Standard. Tony Smollett adds "URM's consultants covered the span between the esoteric (IT) and practical (operations)".

Raising Awareness and Competency Management

As part of its ISO 27001 implementation project, UK Mail adopted a more structured approach to information security awareness training, as well as defining and managing information security competency requirements. Through this more structured approach, UK Mail identified the need for a greater overall awareness, a more formal and consistent general information security induction process and ongoing refresher training, as well as the management of information security competencies for a number of key information security roles identified within the business.

ISMS Operation and Review

Getting the ISMS governance structure right was critical to ensuring that ISMS monitoring and performance measurement worked well for UK Mail. Following URM's suggestion, a dedicated team was established to manage the ISMS at an operational level, with a feed into top management for strategic review. With representation across all areas of the business, the introduction of the Information Security Operational Team enabled direct integration and adoption of ISMS activities within business-as-usual processes. With the new Team came a greater focus on meaningful metrics that directly affect UK Mail's business performance and the achievement of objectives.

Without doubt, URM helped us to achieve our planned objectives a lot sooner than expected. The engagement was a huge success and couldn't have gone any better

Tony Smollet

UK Mail

KEY SUCCESS CRITERIA

Timeline

For UK Mail, implementing ISO 27001 against a backdrop of exceptional and demanding business circumstances was always going to be a challenge. Achieving certification would provide an ideal information security footing for new products, supporting business growth and the planned re-location of its central hub in 2015. A careful balance needed to be achieved between the time needed to develop ISMS maturity, versus the limited window available to capitalise on business opportunity and the need to maintain momentum. URM helped guide UK Mail in its implementation strategy to achieve the optimum balance.

Leadership Commitment

UK Mail established an Information Security Steering Group, comprising four members of its Executive Management Team, to oversee and support the ISO 27001 project, increasing the frequency of information security management review meetings during the implementation period. Close involvement of the Executive Management Team was crucial in keeping UK Mail's ambitious implementation schedule on track.

Coupled with the governance of the Executive Management Team and the recruitment of a permanent information security manager, the active contribution of key senior managers and local champions across the business was also vital in creating a sustainable ISMS.

Regular Communication

Given the geographic spread of UK Mail, regular project communication across the whole of the organisation was of particular importance during the implementation. URM worked in close collaboration with UK Mail's Marketing and Communications Team to keep all employees informed of progress, what to expect and the changes being made.

Awareness and Cultural Change

Prior to implementing ISO 27001, information security had been seen by many areas of the business as being an 'IT issue'. Achieving cultural change and getting everyone to see information security as a business operations issue was one of the project's key success criteria. This cultural change was predominantly achieved through fostering a practical 'plain English' understanding of the many different aspects of information security and a highly successful information security awareness campaign. Real life examples of departmental issues were widely used, along with the promotion of the benefits which can be derived through good information security behaviours.

URM

URM's consultants took time and effort to fully understand UK Mail's culture, environment and priorities, tailoring its implementation approach to work sympathetically with the organisation's risk appetite, capabilities and limitations. During the project, URM were able to offer great resource flexibility, responding to UK Mail's changing resource levels, business commitments and priorities.

Tony Smollet adds "Without doubt, URM helped us to achieve our planned objectives a lot sooner than expected. The engagement was a huge success and couldn't have gone any better."

BENEFITS DERIVED

Business Growth and Customer (Information Security) Assurance

ISO 27001 has provided UK Mail with a strong information security management foundation for developing new products and services, demonstrating and measuring good practice compliance and providing customers with the confidence that their information is in safe hands with UK Mail.

Andy Barber, Head of imail, comments "Obtaining ISO 27001 for the entire UK Mail operation is a significant enhancement for the imail solution. Our clients can now be assured that fundamental data security principles apply equally to both digital and physical forms of their mail communications."

Implementing an ISO 27001 certifiable ISMS has generated efficiencies and consistency for UK Mail when responding to and managing its customers' information security requirements.

Internal Information Security Awareness and Culture

Information security awareness across UK Mail has significantly improved as a result of UK Mail's implementation of ISO 27001. Removing complexity, breaking down the barriers of confusing terminology and adopting a practical approach to information risk management were key cultural enablers in making good information security management part of UK Mail's everyday business and encouraging more open incident reporting.

UK Mail's ISO 27001 implementation project was initially driven as an IT led objective, but through the course of the implementation, UK Mail recognised wider benefits and the project became increasingly business led.

Russell Mannix, Head of Loss Prevention adds "UK Mail's ISMS has become truly embedded and business driven. It supports and facilitates information security best practice across all of our business activities."

Russell Mannix, Head of Loss Prevention at UK Mail

Process Improvement

IT operations and development processes were at the heart of much of UK Mail's control implementation activities. Certification to ISO 27001 created an opportunity to re-prioritise and accelerate many planned activities, as well as making a number of process improvements as a by-product of the ISMS implementation.

Supplier Management

UK Mail maximised the opportunity to improve its supplier management. By implementing mechanisms to manage supplier information security controls, UK Mail further improved its overarching supplier management policy.

NEXT STEPS

UK Mail's next steps are in developing the maturity of its ISMS, reducing information security risks beyond the most significant ones prioritised for initial treatment and focusing on continual improvement supported by an ongoing information security awareness campaign.

UKMail

For more information on UK Mail's services
T: 0121 353 1010
W: ukmail.com

ISO 27001 CERTIFICATION EUROPE™

For more information on Certification Europe's assessment services
T: 0203 0087 818 (Robert Lyons)
E: rlyons@certificationeurope.com
W: certificationeurope.co.uk

URM

For more information on URM's consultancy services:
T: 0118 2065 410
E: info@urmconsulting.com
W: www.urmconsulting.com