

# ISO 27001: Swiss Post Solutions Limited



Swiss Post Solutions Limited (Swiss Post Solutions) has evolved from being the UK's leading provider of outsourced mailrooms to an integrated document outsourcing services specialist with a portfolio of blue chip companies and operations across Europe, the USA, Middle East and Asia.

Formerly known as MailSource, Swiss Post Solutions has expanded rapidly through a combination of organic growth and acquisition. As an independent subsidiary of Swiss Post, the Company provides document, dialogue and e-business solutions to enable organisations to manage their customer interaction effectively and to optimise back-office functions along the document lifecycle.

## Why 27001?

At the end of 2008, the Leadership Team within Swiss Post Solutions was considering its priorities, including ongoing corporate governance, developments and targets for 2009. Included within this, a range of management system and regulation standards were considered as part of a desire to taking a proactive approach to improving the quality of service delivery and providing stakeholders and customers with a statement of intent and commitment. After careful consideration, the Leadership Team selected certification to ISO 27001, the International Standard for Information Security Management, as a priority goal for 2009.

Jonathan King, Chief Executive Officer of Swiss Post Solutions comments "As an internationally recognised standard, ISO 27001 was seen as the ideal vehicle for demonstrating that customer information management is a top priority for us. It lets our customers, partners and prospects know that we take the protection of their data extremely seriously." Charles Parrington-Tyler, Services Director, goes on to add "The name Swiss Post is synonymous with safety, security and efficiency. ISO 27001, with its robust and systematic approach to information security management was seen as highly complementary and a logical step forward."

## Desire to Gain Maximum Benefit from Exercise

One of the fundamental premises underpinning Swiss Post Solutions' decision to seek ISO 27001 certification, was the desire to derive the maximum internal benefit from achieving and maintaining certification. It was certainly not to be a simple box ticking exercise. From day one, it was essential that all relevant

parts of the organisation which would be involved in maintaining the improved security environment were fully involved in the development and implementation of the information security management system (ISMS). It was also paramount that the management system would need to be fully embedded into the organisation and fully integrated with existing management systems. Swiss Post Solutions was adamant that any activities involved in preparing for certification to ISO 27001 would be regarded as 'business as usual' and not treated as a stand alone, independent project that the business inherited at a later date. The Compliance Department, for example, was involved in leading the project and was fully involved in the decision making process including deciding who was responsible for delivering different controls. This participation would enable the department to be more effective in ensuring that the security environment was maintained on an ongoing basis.

## Use of External Consultancy

Whilst deciding that all parts of the organisation were to live and breathe the Standard, Swiss Post Solutions believed it could benefit from the external guidance of an ISO 27001 specialist consultancy. URM, with its extensive certification experience together with its knowledge transfer and training ethos, was felt to be an ideal match and was appointed accordingly.

## Ambitious Timescale

Another fundamental decision involved the timescale. Having decided to start in January 2009, Swiss Post Solutions set the ambitious target of achieving certification by Q4 2009. With full senior management commitment and awareness that the risk assessment phase would inevitably lead to remediation activities from which Swiss Post Solutions could benefit, there was an eagerness to progress as quickly as possible. The Company felt that a challenging timescale would minimise any possibility of there being any loss of momentum.

## APPROACH TAKEN TO GAINING CERTIFICATION

### Workshop

One of the key early influences from URM was to start the project with a 2 day implementation workshop.



As Lisa Dargan, Business Development Director at URM explains, the goals of the workshop were twofold. “One was to ensure the Leadership Team was fully aware of all the activities and resources that were necessary to both gain and maintain certification.

The second goal was to ensure that through an interactive workshop the approach taken to achieve certification was tailored to the Company, maximising any existing approaches or working practices.” Two key outputs from the workshop were the scope of the certification and a high level project plan. In line with Swiss Post Solutions desire for there to be maximum external and internal benefit, it was decided that the whole organisation would be included within the scope of certification. Despite presenting a testing challenge, Swiss Post did not want any customers (existing or future) to be excluded through a partial scope, nor there to be any confusion internally. Swiss Post Solutions found the workshop enormously beneficial with the Leadership Team heavily involved in all key decisions.

### Risk Assessment

The cornerstone of the ISO 27001 Standard is the risk assessment, which forms the basis for prioritising necessary remediation activities. This was another area where Swiss Post Solutions relied heavily on URM’s expertise and experience. Abriska, URM’s purposely designed risk assessment software was utilised and assisted in the identification and prioritisation of risks, along with the generation of an ISO 27001 compliant statement of applicability and risk report. Indicative of Swiss Post Solutions Leadership Team’s commitment to the exercise was the length of debate and discussion that followed the risk report in setting the risk strategy and risk treatment activities. Despite the certification deadline pressures, Swiss Post Solutions was adamant that any strategic decisions were fully debated in order that proposed remediation activities gained total support, were appropriate for the organisation’s culture and were sustainable in the long term.

As Charles Parrington-Tyler explains “For every key decision, the Leadership Team went back to first principles and asked ‘why are we doing this?’ and ‘what benefits are we going to gain?’ It was never a case of we should be doing this merely so we can gain certification.” Thus, following full and inclusive debates a number of significant strategic investment and reorganisation decisions were made. Once the strategy had been agreed, the focus moved to implementation and the key role to be played by the Information Security Forum.

### Centralised Policies and Processes

A key decision made by the Leadership Team was to centralise information security policies and processes across all sites, with exceptions only being made on a customer basis. Having a minimum benchmark and consistency across all parts of the organisation was seen as paramount. Following a number of corporate acquisitions, it was crucial that security practices were consistently adhered to. In order to achieve this, Swiss Post Solutions went to considerable lengths to ensure that heads of all major sites were represented on the Information Security Forum and were involved in discussing and agreeing the approach to policy.

### Local Implementation

It was vital to Swiss Post Solutions that information security was embedded and was everyone’s responsibility and not just that of an information security manager. As such, whilst policies were centrally set, implementation responsibility was assigned locally. A fundamental decision was taken not to appoint a central information security manager but to appoint local, site-based information security controllers. Michael Luff, Compliance Manager at Swiss Post Solutions notes “In order for this model to work it is vital there is strong coordination, trust and communication between the sites.”

## BENEFITS GAINED

On 30 September 2009, Swiss Post Solutions was recommended for certification to ISO 27001. In achieving certification, Charles Parrington-Tyler believes a number of external and internal benefits were maximised. “Gaining ISO 27001 certification is obviously important to Swiss Post Solutions. It provides us with a valuable form of external validation and recognition of our information security management system. It clearly demonstrates to our customers and stakeholders how committed we are to information security, underpinned by robust policies and execution procedures. Furthermore, thanks to the support of URM and the use of its risk assessment software Abriska, we have the added confidence that our security strategy, along with remediation activities, are all based on an objective and impartial risk assessment.” Charles Parrington-Tyler goes on to explain that the actual process Swiss Post Solutions adopted has led to a number of benefits. “At all stages, we involved representatives from all parts of the organisation and believe that the creation of the Information Security Forum has already helped and will continue to help team working, improving communication and local accountability, as well as ensuring information security is truly embedded into our operating culture. In addition, following a review of our business continuity plans we now have a more structured approach to business continuity which is in line with BS 25999 the new Business Continuity Management Standard. Overall, we now have a consistent minimum benchmark standard for information security which can be applied to new acquisitions. Everyone appreciates that this is a journey of continual improvement, but gaining certification to ISO 27001 has given us the ideal platform to build on.”

For every key decision, the Leadership Team went back to first principles and asked ‘why are we doing this?’ and ‘what benefits are we going to gain?’

## Getting the balance right

URM Consulting Services Ltd. , Blake House, Manor Park, Manor Farm Road, Reading, RG2 7JW, United Kingdom

+44 (0)118 206 5410 | [info@urmconsulting.com](mailto:info@urmconsulting.com)