DUAL ISO 27001 & ISO 22301 Certification Case Study

URM

Scottish Friendly

INTRODUCTION & BACKGROUND

Founded over 150 years ago, Scottish Friendly Assurance Society Limited (Scottish Friendly) is the largest mutual life society in Scotland with over 390,000 members and more than £900 million of funds under management. Friendly and mutual societies offer members similar services as banks or insurance companies, with the key difference being that profits generated by societies are retained for the benefit of the policyholders.

Scottish Friendly, particularly in the last 20 years, has gained a reputation for being one of the most progressive financial institutions in the UK. The Executive Management Team has driven innovation in a number of ways in order to streamline the organisation and deliver cost effective and highly responsive, low entry investments and financial products to its members. Such innovations include investment in IT infrastructure and tailored software packages, along with the establishment of a highly successful sophisticated direct marketing, e-commerce and partnership selling operation. Through its forward thinking, Scottish Friendly's Executive Management Team has sought to continually improve efficiencies and service levels to its members.

In October 2013, Scottish Friendly achieved certification to ISO 22301 (the International Standard for Business Continuity Management) having successfully transitioned over from BS 25999, the British Standard. This achievement followed on from attaining certification to ISO 27001 (the International Standard for Information Security Management) in the previous year. As a result, Scottish Friendly joined a small and elite number of institutions that have achieved dual certification against both information security (IS) and business continuity (BC) Standards. This case study shares some of Scottish Friendly's experiences, including business drivers, key success criteria and benefits derived.

Business Drivers

The motivation for many organisations in acquiring certification to ISO 27001 or ISO 22301 is often externally driven e.g. being mandated by a key client as part of contract negotiation. This was not the case with Scottish Friendly. The main driver was an internal desire to adopt best practice and continually improve its IS and BC processes and approaches. As Fiona McBain, Chief Executive explains "Scottish Friendly takes its responsibilities very seriously and attaches great importance in ensuring the confidentiality, integrity and availability of customer information. Providing first class customer service is at the heart of what we do and building upon best practice in all our business operations helps us achieve this." As an organisation which has moved from a direct selling model to direct marketing and more recently and to great effect, e-commerce, there is now a greater reliance and dependence on its IT infrastructure. As such, maintaining the availability of IT systems is critical to Scottish Friendly and hence one of the drivers behind the focus on BC.

> *"Scottish Friendly takes its responsibilities very seriously and attaches great importance in ensuring the confidentiality, integrity and availability of customer information. Providing first class customer service is at the heart of what we do and building upon best practice in all our business operations helps us achieve this."*
>
> Fiona McBain

KEY STAGES & SUCCESS CRITERIA

Scottish Friendly's Executive Management Team, including Fiona McBain, Chief Executive and Jeff Wilson, Head of IT (standing far right).

Senior Management Commitment

From day one, there was total consensus in terms of support from the Executive Management Team for both certification projects. They were always treated as a natural extension of the organisation's desire to:

- Protect the interests of its members
- Avoid any complacency and continually improve its management systems
- Adopt best practice.

Senior management's total commitment to the projects ensured there was a clear, unambiguous message (both internally and externally) as to the importance of IS and BC within Scottish Friendly.

Support of Consultancy Partner and Certification Body

At the start of the certification project, Scottish Friendly realised that it could benefit from the experience and expertise of a consulting and training organisation which had a proven track record of developing management systems in line with the requirements of ISO 27001 and ISO 22301.

Jeff Wilson, Head of IT, comments "Scottish Friendly has a lot of highly capable resources and we were determined to own the development of our management systems. As such, our ideal partner would be one that offered a 'light touch' and 'gentle steering' approach and that is exactly what we got with Ultima Risk Management (URM). The consultant spent considerable time understanding our culture and existing processes before fine tuning and tailoring existing documentation, filling in gaps and assisting in the development of the management system in line with the requirements of both Standards."

British Standards Institution (BSI) was selected as the certification body quite simply for its reputation of being the 'de facto' Standards and assessment organisation.

Scope of Certifications

Given the business objective of adopting best practice across the society, Scottish Friendly believed that the most meaningful scope would be the whole organisation. As Jeff Wilson explained "It was important that an all-inclusive approach was taken where all staff felt engaged in the process. With regard to the Standards, we always saw information security and business continuity as mutually dependent activities with considerable overlap."

Business Impact Analysis and Risk Assessment

Operating in a highly regulated sector, Scottish Friendly was no stranger to conducting risk assessments. Despite this, it still found this stage of the project valuable and benefited from the experience and expertise of URM, particularly in satisfying the requirements of ISO 27001 and ISO 22301.

A combined business impact analysis (BIA) and risk assessment was conducted for both IS and BC using Abriska, URM's purpose designed software. This helped minimise the time demands on managers, as well as producing valuable management reports and all the necessary documentation documentation required by the Standards.

Staff Education and Awareness Programme

Undoubtedly, one of the key stages in the project was the delivery of education and awareness sessions which were attended by all members of staff. They helped to ensure procedures were consistently adopted and followed. Jeff Wilson adds "Staff at Scottish Friendly were already very familiar with awareness initiatives and adding information security and business continuity to the corporate training programme was a relatively simple task. However, the impact was significant as staff became aware of the importance to Scottish Friendly of good information security and business continuity, as well as their individual responsibilities."

Developing Integrated Management Systems

Prior to the start of the certification programmes, Scottish Friendly had already developed a number of effective policies, processes and BC plans. The organisation had always placed great emphasis on treating client information with care and diligence. URM was able to assist in advising on the continuous improvement elements of the management system, ensuring that best practice was continually and consistently maintained. The best example of this was in the integration of the incident reporting process, along with the corrective and preventive procedures. Scottish Friendly initiated an 'Action Tracker' system where staff were encouraged to report any incidents (IS or BC) into one repository so that the Information Security and Business Continuity Committee (IS&BCC) could address all actions together. URM was also able to advise on the fine tuning of the 'Management Review' and 'Auditing' processes so that the requirements of ISO 27001 and ISO 22301 were fully met.

Exercising of BC Plans

A fundamental stage in the development of any business continuity management system is the exercising of BC plans and this was certainly the case with Scottish Friendly. One of the key exercises involved 20% of the workforce relocating to its disaster recovery site located 5 miles from its head office. Apart from the obvious advantage of providing tangible evidence that the BC plans actually work, it also served to raise awareness and confidence of staff that in the event of any disruption they will know exactly what is expected of them. The exercise also served as an opportunity to highlight inter-departmental dependencies and reliance on particular pieces of information.

Forming of IS and BC Committee (IS&BCC)

The flat management structure of Scottish Friendly, combined with an engaged Executive Management Team, has served to restrict the number of committees operating within the Society. In response to the requirements of ISO 27001, an Information Security Committee was created which included two members of the Executive Management Team and line managers from across the organisation. After a few meetings of this Committee, its terms of reference were extended to include business continuity. The IS&BCC was a significant project success, raising awareness of best practice at senior management level and encouraging greater responsibility and accountability amongst staff.

BENEFITS SEEN

Staff Involvement

Whilst there was already a strong IS and BC aware culture within staff at Scottish Friendly, the ISO 27001 and ISO 22301 certification programme served to ensure a greater consistency and involvement across all parts of the organisation. It ensured that IS and BC were embedded within the culture and confirmed all staff's responsibilities and accountability. The BC exercise involved 20% of workforce being relocated to another workplace, it highlighted some logistical issues, but was highly effective in raising awareness amongst staff of what to do in the event of incidents. As a result, staff have taken more ownership and are less reliant on direction from the Head of IT and other members of the IS&BCC.

Reducing Preparation Time for Auditing

Operating in a highly regulated market sector, Scottish Friendly is naturally subject to numerous external audits. The introduction of modifications and improvements to the management system has helped to reduce some of the audit preparation time and face-to-face contact with auditors, as many of the processes and activities established to meet the requirements of the two Standards are easily recognisable to auditors. It has also ensured that audit activity is a more inherent part of business life and is engrained in the organisational culture.

Improved Feedback Mechanism

The introduction of the integrated 'Action Tracker' incident reporting and incident management system has helped to streamline and simplify the corrective and preventive action procedures.

More Resilient and Better Prepared for Disruptions

Overall, the organisation feels that through the introduction of a more formal programme it is better prepared to initially avoid disruption and, in the event of an incident, to minimise any disruption.

Information Classification and Handling

Whilst Scottish Friendly had processes in place for the handling and management of client information, it had not extended those processes to its own internal information. The introduction of an organisation-wide 'information classification and handling process' addressed this and encouraged staff to be more aware of and to consider how best to transmit information externally.

Scottish Friendly

W: www.scottishfriendly.co.uk
T: 0333 323 5433
E: enquiries@scottishfriendly.co.uk

URM

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

bsi.

For more information on certification to ISO 27001 with BSI:
T: 0845 080 9000
W: bsigroup.co.uk/infosec