



**FIRE
DO NOT CROSS**

ISO 27001 Case Study

Cambridgeshire Fire & Rescue Service

'Fire prevention' in the world of information security!

Background

In April 2008, Cambridgeshire Fire & Rescue Service (CFRS) became the first fire and rescue service in the UK to gain certification to ISO 27001 the international Information Security Management System (ISMS) Standard. This case study highlights some of the key stages that CFRS went through in achieving certification along with the lessons it learnt and what it considered to be the critical success criteria.

CFRS provides professional fire and rescue services to over 700,000 people in Cambridgeshire and the city of Peterborough. The vision of the Authority is that:-

"In order to become a key contributor to community safety it is necessary to proactively identify risks and take positive action to save lives, protect people and safeguard the environment."

This proactive and positive approach is exactly what CFRS has adopted to preserve the confidentiality, integrity and availability of information it holds. Like many other fire and rescue services, CFRS stores and processes some highly confidential information as well as being dependant on the analysis of its data, such as incident management statistics, to improve its operational performance.

Thanks to the original vision of Martin Scott, a previous Resources Director, CFRS identified ISO 27001 as being the ideal framework around which it could develop and improve its ISMS.

Business Challenge

As CFRS saw it, any ISMS developed "had to address a number of business issues and challenges. What was critical, was to ensure anything produced was aligned to meeting business goals and something that was first and foremost risk-based".

At the same time CFRS was mindful of meeting:

- Its legal obligations, notably complying with the Freedom of Information Act 2000 and the Data Protection Act 1998
- The requirements of the Audit Commission who regularly conduct Comprehensive Performance Assessments
- Security related issues raised by internal auditors
- The needs of internal users by providing support to drive the improvement of internal services.

ISO 27001 - A Business Solution

One thing the Senior Management of CFRS all agreed upon was that the Service was not looking for a 'quick-fix, short-term solution'. As Graham Edridge, Data Protection Adviser and ISMS Project Manager at CFRS explains "We wanted a long-term solution which was based on continuous improvement. This was why we were so attracted to ISO 27001 with its 'Plan, Do, Check, Act' model of continuous improvement. We also wanted a management system which was truly embedded into the organisation" Julian Thrussell, Product Marketing Manager for BSI Management Systems UK agrees adding that, "Whilst implementation of an Information Security Management System will not guarantee against security lapses it certainly means that their potential and impact will have been assessed and that suitable controls will have been put in place to limit any potential breaches. The ISO 27001 Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the management system."

Key Activities

Setting the Scope

CFRS recognised early on that the first step in the journey was to ensure the scope of the project was something which was both meaningful and manageable. The decision was to focus on the ICT Function. Although ICT staff only accounts for a small percentage of the overall CFRS workforce, the information and information processing assets extend into virtually all areas of the organisation. This meant that 30 sites were included in the ISO 27001 scope, including a number of retained fire stations, which are not always staffed.

BIA and Risk Assessment

Having set the scope and determined the relevant asset groups, CFRS recognised that it had to identify and calibrate all information security risks before it could prioritise and implement the relevant controls. Graham Edridge takes up the story. “We were keen to utilise the skills and experience of a consultancy that had a proven risk assessment methodology and were fully conversant with the ISO 27001 Standard and the certification process. However, just as important, we were determined to acquire as much knowledge as possible through formal training and activity shadowing. That’s why we chose Ultima Risk Management.”

The risk assessment that was conducted included business impact interviews with senior decision makers which ensured that risks were aligned with business goals. The risk assessment also assessed the likelihood of threats and the vulnerability to threats. The outcome of the risk assessment was a prioritised list of actions. “What was reassuring” comments Lisa Dargan, Business Development Director at Ultima Risk Management (URM), “was that the findings generally concurred with the Audit Commission and internal audit findings.” In conducting the process, CFRS adopted Abriska 27001 URM’s automated risk assessment tool. A major feature of Abriska 27001 is that risk assessment questions can be distributed out to the most appropriate contacts throughout the organisation. Enabling multiple users to concurrently work on questions led to considerable time savings for CFRS.

Risk Treatment

One of the outputs from Abriska 27001, was a prioritised Risk Treatment Plan (RTP) which identified areas requiring immediate attention, notably “the need to develop stronger, up-to-date policies and the need to identify and document all ICT operational procedures. In particular, there was a strong need to introduce more robust processes and documentation within the Help Desk facility, i.e. improving processes around issue resolution, asset registers, and change control.” With

URM’s assistance, CFRS developed and implemented a comprehensive set of policies including an overarching Information Security Policy. One of the key supporting policies created was an Information Security Event Reporting and Management Policy which classified security events into separate categories. At the same time as introducing a new set of policies and procedures, CFRS invested in a document management system which allowed the document management controls within ISO 27001 to be adhered to.

Security Awareness Campaign

A key component of the risk treatment phase was the development and delivery of a security awareness programme. This was a critical activity in terms of facilitating the necessary culture change. The challenge for CFRS was how to communicate with a diverse workforce which was spread over 30 sites and which encompassed different shift working patterns. CFRS achieved this with a multi-pronged approach including producing information packs, laminated wallet cards and targeted awareness training to different groups in the Authority. All of the training and promotional material was uniquely branded in red and black with an easily recognisable logo which the Service designed in house, helping to ensure that it stood out from other corporate messages. At the same time, information security training was integrated into existing business structures and delivered by the CFRS training department, thereby avoiding any additional overhead expense being incurred.

Ongoing Improvement

From the first day CFRS recognised that ISO 27001 was not a one-off exercise but represented a commitment to a continual improvement programme. As part of this commitment, CFRS invested in Abriska 27001 which has enabled it to conduct risk assessments in a consistent and cost effective way. CFRS utilises the number of actions coming out of the RTP as one of the ISMS performance measurement metrics.

As part of the monitoring and reviewing process, CFRS established an Information Security Forum (ISF) which meets every two months and addresses specific actions originating from the RTP. The Forum also reviews the number and nature of incidents being reported along with corrective and preventive actions. In addition to the ISF, information security is a regular agenda item at Management Review meetings where quantitative and qualitative information is presented to senior management. These meetings have proved extremely effective at resolving issues where senior management involvement is necessary to removing any ‘pockets of resistance’ to the adoption of new working practices.

Critical Success Criteria

Graham Edridge has identified a number of key factors which contributed to the success of the ISO 27001 certification programme.

Planning and Communication

“We spent a significant amount of the project time on planning ahead of implementation and this has greatly helped us avoid many of the common pitfalls. A lot of time also went into understanding the issues and communicating objectives and benefits as simply and clearly as we could to users.”



Senior Management Team Involvement

“Absolutely key to the success of the project was, and is, the support and encouragement provided by the Senior Management Team. Information security is now a regular feature of management review meetings and there is a genuine appetite for ongoing improvement and addressing security issues.”

Knowledge Transfer from External Consultancies/Certification Bodies

“We found the expertise and experience of organisations like BSI and URM invaluable in guiding us. The fact that both were so willing to transfer knowledge was critical in the development of our own skills and our own self sufficiency. I would also personally recommend that organisations consider attending training courses ahead of embarking on any ISO 27001 certification programme.”

Integrating into ‘Business as Normal’

“It is essential that information security is seen as a normal everyday activity and this has been achieved by utilising the training department to deliver information security awareness sessions and including information security as a regular agenda item at business meetings.”

Security Awareness

“Linda Walkden, the Projects and Network Coordinator at CFRS, worked with the in-house Design and Communication Officer Sophie Binding to create some very distinctive branding for our promotional and awareness training material (a logo, posters, leaflets, information packs and wallet cards) which gave the whole campaign a coordinated, professional and consistent feel as well as adding to the impact of the messages.”

Automated Risk Assessment Tool – Abriska 27001

“Through the adoption of Abriska 27001, we now have a thorough and repeatable risk assessment methodology. Having used Abriska, I just couldn’t contemplate the thought of going back to a manual process!”

Dedicated Resource and Specialist Training-

“Having a dedicated resource (Linda Walkden, Projects and Network Coordinator) with me providing back up has really helped maintain a momentum through the whole programme. We both attended ISEB accredited information security and risk management training courses with URM and this helped to put ISO 27001 into the context of information security as a whole”.

Getting Scope Right

“With hindsight, I do feel that we got the scope of the ISO 27001 certification just about right. A scope that was meaningful and challenging but achievable. Our BSI assessor was a great help here helping us decide what was in and out of scope. What was useful was to graphically represent the boundary helping internal staff to fully understand all of the information flows.”

Benefits Seen

Improved Security Environment and Greater Transparency

Graham Edridge believes ISO 27001 has provided 'a great framework' around which information security can be built. "It has certainly led to a tangible difference in the organisational culture. There is, for example, a far more open and transparent environment in the reporting of security events or breaches. This is absolutely key if we are to be effective in implementing corrective and preventive actions."

Stronger Policies and Operational Procedures

One of the key risk treatment activities was the need to develop stronger, up-to-date policies and the need to identify and document all ICT operational procedures. In total CFRS' Information & Communications Technology (ICT) Group has published 23 new information security policies including the key CFRS Information Security Policy. This 2 page document has been pivotal in communicating the high level information security objectives to all staff.

The documentation of ICT operational procedures has also been extremely beneficial in helping the Service to

reduce the risks associated with information being held in heads and 'single points of failure'.

Role Model

By becoming the first fire and rescue service to achieve certification CFRS has established itself as a role model for other fire and rescue services to follow. In the same way that CFRS benefitted from learning from URM and BSI so CFRS started providing other fire and rescue services with the benefits of its knowledge. CFRS has presented the benefits associated with ISO 27001 to the national Chief Fire Officers Association ICT Managers Group and has hosted an ISMS Conference for Fire and Rescue Services throughout the country at the Service HQ in Huntingdon.

Good Corporate Governance

Senior management is aware that it can never have a 100% secure environment. What ISO 27001 certification does provide, however, is the 'peace of mind' that CFRS has committed to an ISMS which is risk based and built on continuous improvement. In doing so, the Authority has taken a proactive approach to minimising the risk of security breaches occurring.

Selecting Key Partnerships

Ultima Risk Management (URM)

Partnering with URM led to a number of benefits notably:

- The knowledge transfer philosophy of URM combined with its formal ISEB training course and qualification offerings were critical in the development of in-house skills and knowledge. Members of the ICT Function attended URM's 'Certificate in Information Security Management Principles' and 'Practitioner Certificate in Information Risk Management' courses.
- URM's Abriska 27001 tool has proved an invaluable asset to CFRS in conducting risk assessments and is key to improving the ISMS. Through its centrally managed BIA/RA methodology, CFRS can guarantee consistency of approach to questionnaire completion and terminology interpretation. The organisation has also integrated some of the reports from Abriska into its metrics for measuring the performance of its ISMS.
- With URM's assistance, CFRS was able to, more quickly and efficiently develop and implement a comprehensive set of policies including an overarching Information Security Policy. This latter document is key in the communication of information security objectives to all staff.

BSI Management Systems UK (BSI)

The selection of BSI as the chosen certification body led to a number of benefits:

- CFRS found the pre assessment visit from BSI hugely helpful in understanding the certification process and what the assessor would expect to find at both Stage 1 and Stage 2. BSI also played a key role in setting the scope for certification.
- Whilst being very rigorous in assessing CFRS' ISMS, Graham Edridge found the BSI assessor to be "patient, and prepared to go the extra mile in providing constructive and encouraging feedback on the development of the ISMS."
- CFRS ICT found a number of the assessment techniques very useful in developing its own internal audit and review activities.

For further information please contact Ultima Risk Management Ltd

Tel: 0118 902 7453 Email: info@ultimariskmanagement.com Web: www.ultimariskmanagement.com