

ISO 27001



'Fire prevention' in the world of information security!

Background

Cambridgeshire Fire & Rescue Service (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 be 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 the 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 dependent on the analysis of data such as incident management statistics to improve its operational performance.

Thanks to the vision of Martin Scott, Resources Director, the CFRS identified ISO 27001, the International Standard for Information Security Management, as being the ideal framework around which it could develop and maintain its Information Security Management System (ISMS).

Business Challenge

As Martin Scott 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 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 the 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", comments Martin Scott, "was that we were not looking for a quick fix short term solution. 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."

Scott Hanney, Key Account Manager at the British Standards Institution (BSi) agrees, *"The concept behind ISO 27001 really is very straight forward; identify the business need, implement the relevant controls and ensure these controls are maintained and, if necessary, improved."*

Journey So far

CFRS recognised early on that the first step in the journey was to ensure the scope of the project was something which was manageable. For this reason it was decided to focus initially on the ICT Function. It was also recognised that it had to identify and calibrate all information security risks before it could prioritise and implement the relevant controls. Graham Edridge, Data Protection Adviser and ISMS Project Manager at CFRS 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. That’s why we chose Ultima Risk Management.”*

The risk assessment conducted included business impact interviews with senior decision makers and ensured that risks were aligned with business goals. The risk assessment addressed threats from vulnerability and likelihood perspectives. The outcome of the risk assessment was a prioritised list of actions. *“What I found reassuring”* comments Nicola Hope, Senior Security Consultant at Ultima Risk Management (URM), *“was that the results generally concurred with the Audit Commission and internal audit findings.”*

From Graham Edridge’s perspective the risk assessment and the resulting Risk Treatment Plan identified some areas requiring immediate attention, notably *“the need to develop stronger, up-to-date policies and to identify and document all ICT operational procedures. In particular, there was a strong need to introduce stronger 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 has implemented a set of key policies along with clear ownership and robust review processes, in addition to making real inroads into improving the security awareness of staff though the organisation. This is no mean achievement when one considers the split 24/7 working shifts and a service based over nearly 30 sites.

Benefits seen to date

What about certification? *“This is a very important goal for us.”* comments Graham Edridge, *“Gaining certification will greatly reassure our external*

stakeholders that CFRS’s ISMS has been validated and audited by an independent certification body like BSi. What is really positive though are the practical benefits we are experiencing purely by going through the process of complying with this Standard and developing our ISMS.” Benefits which CFRS have already seen include:-

- Stronger operational procedures notably in the Help Desk areas leading to improved security and service to internal users
- Greater clarity and simplification of policies
- Greater awareness of information security throughout the whole organisation

In addition this project has already provided a level of reassurance to senior management that ICT has a clear and holistic view of the key risks and that each additional control being implemented is adding to the security infrastructure.

Lessons learnt to Date

Graham Edridge is clear about the factors which have contributed to the successful running of the project to date.

- 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 to users in order to obtain widespread acceptance.”*
- Senior Management Buy-in *“Absolutely key to the project is the support and encouragement provided by the Senior Management Team, particularly to the concept that this is an on-going project based on continuous improvement.”*
- Dovetailing with external consultancies/ Certification Bodies *“We have found the expertise and experience of organisations like BSi and Ultima Risk Management invaluable in guiding us. The fact that both are so willing to transfer knowledge is critical as we develop our own skills and our own self sufficiency.”*

GETTING THE BALANCE RIGHT.

URM

ULTIMA RISK
MANAGEMENT

Ultima Place, 448a Basingstoke Road
Reading, Berkshire, RG2 0RX

Phone: 0845 838 2084
Fax: 0118 902 7451
www.ultimariskmanagement.com