

Case Study: ISO 27001 Consultancy



NHS Fife Creating IS Awareness

In 2005, NHS Scotland issued the NHS Scotland Information Security Policy. The document was prepared by the Scottish Executive Health Department and is applicable to all Scottish NHS Bodies and their departments.

The NHS Scotland Information Security Policy is based on ISO 27001 (then BS7799), the international standard for establishing, operating and maintaining an Information Security Management System (ISMS) and forms the baseline standard for NHS bodies.

Violet Bolton, IT Services Continuity Manager at NHS Fife had developed a number of policies in line with the recommendations outlined in the document. Violet wanted to communicate the policies throughout the rest of the organisation.

It was decided that NHS Fife would engage a 3rd party to provide Information Security (IS) Awareness workshops to employees to ensure that these policies were communicated effectively throughout the organisation.

NHS Fife approached Sapphire to facilitate the IS workshops. Sapphire came highly recommended from numerous public sector organisations in Scotland and they themselves were certified to ISO 27001 which gave the staff at NHS Fife confidence in their ability to raise IS awareness throughout the organisation.

"NHS Fife had already recognised the need to create a IS culture throughout the organisation," comments Violet Bolton, IT Services Continuity Manager. "We were unsure how to drive this forward internally and therefore enlisted the help of Sapphire. The IS workshops provided by Sapphire's consultants enabled our staff to understand the relevance of the standard to their individual roles and departments."



Study Facts

Customer:
NHS Fife

Website:
www.nhsfife.scot.nhs.uk

Industry:
NHS

Profile:
NHS Fife enlists Sapphire to help them to achieve compliance to ISO 27001 and revise their existing Business Continuity and Disaster Recovery Plans following guidelines published in the NHS Scotland Information Security Policy.

Services:
ISO 27001 Consultancy

Whilst providing the workshops to the staff at NHS Fife, it became apparent to Violet Bolton and her team that it would be sensible to formalise the existing policies and develop extra policies in line with the Information Security Policy document. The project of implementing an ISMS into the scope of the IT function was agreed as a practical and sensible starting point.

The mandatory functions of an ISMS were implemented as a matter of course during the project.

During the process, the project managers had full buy in from the IT Department as this was where the need for the new procedures had originated from.



Finally, by deploying policies and ensuring that the organisation was compliant with ISO 27001, NHS Fife was able to review its existing Business Continuity Plans (BCP) and Disaster Recovery plans (DRP). To assist with the review of the BCP and DRP, Sapphire scheduled a programme of BCP / DR Gap Analysis workshops.

"The Gap Analysis workshops enabled us to establish our current state, agree on practical steps going forward to improve NHS Fife's existing BCP / DR procedures and to bolster the overall resilience of the organisation."

Comments Violet Bolton. "Sapphire's consultants contributed to the workshops; guiding our team throughout the process and offering advice in the areas in which we struggled."

NHS Fife is working in compliance to ISO 27001 having successfully undertaken a mock compliance audit and proving that they have established a compliant ISO 27001 document set. NHS Fife is now in an excellent position to achieve certification to the standard in the future.

Sapphire and NHS Fife are currently working together in order to plot a milestone plan to gain certification and are busy planning a number of ISO 27001 specific workshops going forward.

When asked to comment on the project, Violet Bolton IT Services Continuity Manager at NHS Fife said

"In less than twelve months, an effective and tailored ISMS Framework has been established within NHS Fife IT Department. This timeframe is small in relation to the deliverables established and the noticeable improvements made to the Information Security Culture. Notable achievements being:-"

- Formal Personal IS Policy & associated staff booklet.
- ISMS deliverables especially the Risk Register & the Information Security Manual
- Continuous monitoring mechanisms in respect to the incident management process