Business Improvement Service

Business Improvement – White Paper 18

Strategic
Safety Systems

So, you want ISO 27001 – Information Security Management

By Phil Chambers BSc, CMIOSH

Organisations who handle information, in any format, on other companies or personnel have a duty to securely manage that information. One hears of memory sticks or notebook computers containing details of many people being lost. In addition, unless suitable precautions are taken, it is possible to hack into a company's server and gain access to such information.

Whilst information can be securely managed without any need to be certified to ISO 27001, being certified to this standard shows that a company has robust systems in place which are periodically audited by a third party. Because of this, many organisations require companies to be ISO 27001 certified as a condition of the contract.

Benefits

As a result being certified to ISO 27001, a company will:

- Have systems in place to securely manage information
- Be in a strong position to gain business where information handling is a key part of the business

So what is ISO 27001 and how do we go about getting certification?

ISO 27001 is an information security management standard. Note that it is <u>management</u> standard, not a <u>performance</u> standard. So it is not a just matter of doing the right thing; it is also how you approach that in an auditable, sustainable and improving way.

Essentially there are two steps to gaining certification:

- Setting up and implementing management systems to cover the clauses in the ISO 27001 standard.
- Being audited by a UKAS-accredited certification body. This requires initial certification visits and then repeat visits to maintain certification.

Note that UKAS is the organisation that controls certifying bodies. Beware of companies who are not UKAS-accredited but who claim to be certification bodies. Any certificate will be meaningless.

So how do I go about setting up and implementing management systems?

Before we go any further, I'd just like to recommend that your documentation should be implementation-based. What I mean by this is that it should be written from the perspective of the users of the different systems and not look like semi-legal documents. I recommend the following:

- Use flowcharts wherever possible. A system comprising a couple of pages of flowcharts is far more understandable that multiple pages of, "The Production Manager, on receipt of ……". Flowcharts are just as acceptable to the certification body.

- Where text is necessary, write it in the form of an instruction to whoever is carrying out the action and possibly in tabular form. So, in one column you may have "Security Co-ordinator" and in the next "Register all people who have access to secure information."

- Avoid text like "The Environmental Co-ordinator shall ….". Sometimes it's unavoidable, but minimise it.

- Be concise. You are not being judged on your weight of documentation, just that it covers the relevant ISO 27001 clauses and how well it is implemented.

Scan with RedLaser