So, you want ISO 27001 – Information Security Management

Strategic Safety Systems

Business Improvement Service

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 and practices 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 management standard, not a performance 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 "Assess security risk"
- Avoid text like "The Security 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.

What systems do I need?

Core systems

There is a standard core of systems that you need for ISO 9001, 14001 or 27001. If you already have certification to at least one of these standards, the only work necessary is to add appropriate references to ISO 27001. Such systems include:

- Management review
- Roles and accountabilities
- Objectives and targets
- Training
- Documentation
- Documentation control
- Evaluation
- Non-conformances
- Audits

Systems specially for 27001

The following systems are also required for ISO 27001:

- Information security policy
- Security screening
- Executive acceptance of risk
- Security risk assessment
- Physical security
- Electronic security including access
- Protection against malicious code
- Network security
- Media handling
- Exchange of information
- Incident reporting and follow-up
- Technical vulnerability management

Security risk assessment

This is a key step as this is the tool which identifies the vulnerabilities within the organisation, how they are controlled and what actions are require to improve or maintain control. Event types include:

Event type	Example
Loss of confidentiality	Information become available in the public domain whilst the company's possession
Loss of integrity	Information becomes damaged with no risk of it becoming available in the public domain.
Loss of availability	Information is destroyed or permanently lost with no risk of it becoming available in the public domain.

Note that the SSS INTACT action management system includes a module that simplifies the risk assessment process.

Implementation

People's time

By far the most important part is getting the right people on board as early as possible. You will need someone to take the role of security co-ordinator; don't worry, it should not take up this person's time much but it is important to have someone who keeps things ticking over.

Secondly, management must be committed to the process. You will need to have the occasional management meeting, but dependent upon the scale of your operations, this may be as little as one every 6 months.

Technical vulnerability management

New threats appear regularly and it is necessary to a have provisions in place for keeping up to date with such developments and ensuring that the company's provisions are kept updated to counter such threats.

Making it all palatable

Without a doubt, the stages of setting this up from scratch require quite some effort and companies take one of two routes:

1. Appoint someone internally and they work on this full-time
2. Use external sources to set up the systems and carry out most of the initial work and then use internal people to run the system in additional to their prime role

If route [1] is taken, then it is probably acceptable to have systems that require some effort to track any data. However, most companies do not have the luxury of having such a person.

If route [2] is taken, then provided that a sensible approach is taken to data management, the tasks to run the system should not be at all onerous.

Strategic Safety Systems Ltd., 8 The Highgrove, Bishops Cleeve, Cheltenham, GL52 8JA, UK
Phone: 01242 679713 Mobile 077680 11667
E-Mail: info@StrategicSafety.co.uk Web site: www.StrategicSafety.co.uk