ISO 27001 – AN INTRODUCTION

What is ISO 27001?

The family of standards for ISO 27000 is made up of many documents that refer to correct terminology, how to setup an information security management system, how to implement security using good controls and so on. In this short article we focus on 27001.

Its full name is ISO/IEC 27001:2005 - this is the Information Security Management System requirement standard. Following the standard will greatly enhance security.

So does it apply to our organisation?

The simple answer is yes! Security and observing good security practice applies to all organisations. In some cases failing to demonstrate standards in security can lead to a lack of confidence in an organisation or even loss of clients.
We are usually approached by two broad groups of people - those that just want to get certified and those that want to improve security and in doing so meet the standard.

How does it apply to this sector?

If the standard is followed there will be a marked improvement in Confidentiality, Integrity and Availability (CIA). These areas can be used to measure the level of quality of Security in a typical organisation. Organisations that meet the standard have been through a rigorous process and in doing so have probably made many improvements.

If you have a need to manage risk in your organisation, improve client confidence or generally keep your security model robust and current then you should be looking to a standard to help achieve this.

What if I see an ISO ‘badge’ what does it mean? Should I do business with them?

The truth is that some organisations will get the badge (or ‘a badge’ that looks similar) just to do business or win tenders. Unfortunately not every organisation out there follows their standards through a proper process. An example would be an independent auditing consultancy that takes you through a standard ‘unofficially’ and then issues its own certification to you - how much would that be worth?

Our advice is always to look for standards that are government approved (UKAS - United Kingdom Accreditation Service) and also to ask for examples of how the standard is met in day to day work - the basic requirement is that the company should be audited by UKAS which is an independent approved body.

How do we achieve the ISO 27001 standard?

There are a number of steps, here is a brief summary:

Introduction

You should review at a simple level what security or standards are in place at present and what needs you really have. At this stage take a little time to discuss your security requirements and read up on ISO 27001 - how could it help you? If you have enough technical know-how in house you could even contact the certification body direct to get some advice; alternatively a good security consultancy would guide you through the process and make these actions on your behalf. Additionally, you should collect any documentation you have that is related to security and risk, including Business Impact Analysis (BIA) and documentation of systems and processes.

Step 1 - Internal Audit (GAP Analysis)

Have an ISO 27001 internal audit. This is essentially a GAP analysis stage (Where are we? And where do we want to be?) where a consultant or member of staff will work through the areas in the standard and create an evidence file and a set of responses to the points in the standard.

Step 2 - Implementation

The end result of Step 1 (GAP analysis) is used to formulate an implementation plan which details what needs to be done to improve or reach the required level. It's important to note that some aspects of the standard will not necessarily apply. The ISMS (Information Security Management System) is also established during this stage – the ISMS is usually comprised of a set of documents. Some people prefer to implement it using a package or online service e.g. Microsoft Sharepoint.

Step 3 - UKAS Approved Audit

Now that the organisation is ready you would contact an approved certification body to review the ISMS and perform a formal audit. The results of the audit will indicate any required areas of improvement or comments which should then be worked upon. The follow up audit will take place once any shortcomings have been met.

Step 4 - Approval and Maintenance

At this stage you would expect to receive an official certificate stating the details of the standard and the expiry date. The UKAS auditor would need to be fully satisfied in order to have reached this stage. Also important is to schedule in regular maintenance or surveillance visits from the security consultant that performed the initial audit or implementation. Usually these visits will take place once or twice a year with a fuller assessment every three years.

Costs

Typically you could pay anywhere from £400 up to £900 per day for a good security consultant for the internal audit and depending on the size and complexity of the organisation the official UKAS audit cost will vary with daily rates ranging around the £700 to £900 mark.

The largest cost is often the implementation of the actual standard as it may require more equipment and configuration. It’s also important to consider the time investment factor, staff training and use of new systems may have an impact in the short term on productivity as well as confidence. In the long run however the benefits will outweigh the costs for most organisations.

In Summary

ISO 27001 is a great standard that has been used as the basis for major improvements across all sectors. To reach and maintain the standard will ensure that the organisation is following best practices in all areas. It also leads to a robust and improved service to end users - both internal users as well as the clients of the organisation itself.

Source : http://www.ictknowledgebase.org.uk/iso27001explained