IMPLEMENTING AN ISMS

A REALLY QUICK INTRODUCTION

April 2013

Protect • Comply • Thrive

IMPLEMENTING AN ISMS

A REALLY QUICK INTRODUCTION

What is an information security management system?

An Information Security Management System ('ISMS') is a systematic approach to managing confidential or sensitive company information so that it remains secure (which means available, confidential and uncorrupted). It encompasses people, processes and IT systems.

What is the ISO27000 family of standards?

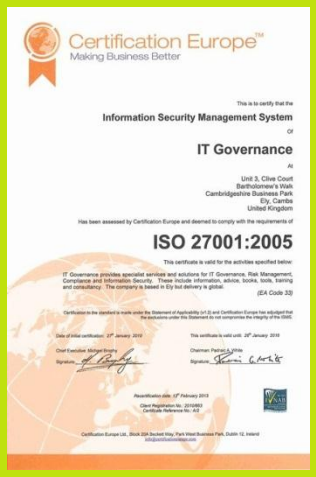
It is a comprehensive collection of standards providing guidance on many aspects of implementing an ISMS. Full details on the ISO27000 standards can be found on our ISO27000 family of standards webpage.

The two standards that are more important for you ISMS project are:

ISO/IEC 27001:2005 is the international standard for information security management – the statement of what should be in an ISMS and the requirements against which it can be audited and certified.

ISO/IEC 27002:2005 is the specification for the design of an ISMS – the how to make it work, not the details of what should be in it. It offers practical guidance on initiating, implementing, maintaining and improving an ISMS.

Information security is not just about anti-virus software, implementing the latest firewall or locking down your laptops or web servers. The overall approach to Information Security should be strategic as well as operational, and different security initiatives should be prioritised, integrated and cross-referenced to ensure overall effectiveness.


Certification Europe
Making Business Better

Information Security Management System

IT Governance

ISO 27001:2005

Example of an ISO27001 certificate – awarded once an ISO27001-compliance ISMS has been externally audited and certified by an accreditation body.

An Information Security Management System helps you coordinate all your security efforts – both electronic and physical – coherently, consistently and cost-effectively.

Implementing an ISMS

There is a standard approach toward implementation of an ISMS that is recommended by BSI and other international certification bodies.

What is absolutely essential is to use suitably competent and trained personnel to implement and manage your ISMS - either consultants or internal staff with appropriate levels of training.

We have provided a representation (together with links to the appropriate ISO standards or IT Governance tools) of it in this paper.

Step 1: Purchase and study a) the Standards and b) Nine Steps to Success – An ISO 27001 Implementation Overview.

If you or any members of staff working on the project have not yet completed ISO27001 training, the following two courses will be of use:

- ISO27001 Foundation
- ISO27001 Lead Implementer

Step 2: Assemble a team (including consultants if appropriate), agree project strategy and the ISMS scope. At this point, you may find IT Governance – an International Guide to Data Security and ISO27001/ISO27002 helpful.

Step 3: Develop an asset inventory as well as a risk assessment and treatment strategy.

vsRisk is a standalone piece of software that can guide your organisation through the process of completing an information security risk assessment compliant with ISO27001.

Step 4: Draft a Statement of Applicability and supporting policies and procedures and get board approval.

Throughout steps 2 and 3, you will be greatly helped by the ISO27001 Documentation Toolkit, which contains all the documents you need in a template format – saving you hours of time during the most labour-intensive part of the process.

Step 5: Implement the ISMS, develop incident response procedures and provide training across the organisation. IT Governance offers a full range of training courses and staff awareness aids:

- ISO27001 e-learning staff awareness course
- ISO27001/ISO27002 pocket guide
- Training aids

Step 6: Monitor, review, check and audit – ensuring that the ISMS works as planned.

Identify and implement improvements prior to seeking (if appropriate) external certification.

These steps fit within what is known as the Deming, or PDCA (for Plan-Do-Check- Act) cycle, which ISO270001 requires to be applied in developing an ISMS.

To become certified, the ISO27001 standard requires at least one member of staff to be competent in carrying out an internal audit. They will need to take this training course to achieve this:

- ISO27701 Internal Auditor Training

A more in-depth 'ISO27001 Lead Auditor' training course is also available.

How long does it take to implement an ISMS?

The answer to this question depends on many factors, including:

- the size and complexity of the organisation,
- the level of management commitment to the project,
- the organisation's underlying preparedness,
- the organisation's current security posture,
- the level of expertise deployed in the project,
- the organisation's existing quality management culture.

For a mid-sized organisation, using the tried and tested IT Governance approach outlined above, certification could be achieved in 4 to 8 months.

For smaller organisations with a single site and fewer than 19 people, we offer a **'Fast-Track'** service. This service has a set price and can get the organisation certification ready in just three months.

Visit our website to find out more.

Challenges in creating the ISMS

Traditional approaches to implementing an ISMS are usually sequential. The companywide 'Plan' phase of the project is completed before the 'Do' phase commences, and neither 'Check' nor 'Act' usually start until after the 'Do' phase is finished.

Within each phase, it's not uncommon for controls to be tackled sequentially; for example, first the anti-virus policy is developed and approved, then the anti-virus procedures, followed by the detailed anti-virus work instructions. Once the work instructions are developed, software is rolled out/adjusted, staff are trained, and then you hope to move on to the next control.

But that's not all there is to the first procedure: it's also got to deal with spyware, worms and Trojans, it's got to integrate with the incident response and business continuity processes, as well as the user access agreement and training aspects of the ISMS.

In total ISO27001 lists 134 controls, each with a similarly complex set of challenges. It is a common misconception, however, that each of the 134 controls must be applied. On the contrary, you only need to apply those controls which are relevant to your organisation and are deemed appropriate upon the outcome of your risk assessment.

This makes the risk assessment process critical in determining what controls to apply.

And if you're doing this through a traditional trial and error approach, you've got to work out for yourself how to get it right across the board.

The IT Governance Toolkit approach

You will want to tackle your project in one of two ways: either area by area (e.g. control by control, or division by division) or across the board. In either case, you need to be sure that there are no cracks in your ISMS.

The IT Governance Complete ISMS Toolkit supports both a sequential mini-PDCA approach and a massively parallel approach. In either case, the templated documents deliver consistent, aligned, coherent policies and procedures that effectively meet the complex, cross-referential requirements of the standard.

Deploying the IT Governance Complete ISMS Toolkit ensures that you meet your project objectives with the minimum of hassle and the maximum of coherence.

Resources for your ISO27001 project

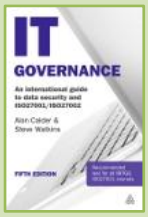
The official ISO/IEC standards documents – reading and understanding these documents is an absolutely essential starting point for an ISO27001 project.

You can purchase all of them from our site:

www.itgovernance.co.uk/shop/c-233-standards.aspx

The IT Governance ISO27001 No3 Toolkit – save yourself hundreds of hours of researching and drafting with this complete toolkit containing documentation, copies of the most relevant standards (ISO27001, ISO27002, ISO27031 and ISO27035), the book 'A Manager's Guide to Data Security', a copy of vsRisk (the leading Risk Assessment tool) and 12 months of updates and drafting support

www.itgovernance.co.uk/shop/p-970.aspx



IT Governance - An International Guide to Data Security and ISO27001/ISO27002

This is fifth edition of THE definitive guide to ISO27001 and ISO27002 compliant information security and management.

www.itgovernance.co.uk/shop/p-772.aspx

Information Security Risk Management for ISO27001/ISO27002

Get practical advice on the implementation and development of an ISO 27001 (ISO27001) and ISO 27002 (ISO27002) compliant information security and risk management system.

www.itgovernance.co.uk/shop/p-607.aspx

ISO27001 Pocket Guides Complete Set

This complete set of ISO27001 Pocket Guides provide an overview of information security best practice & guidance, that is fully aligned with ISO 27000 range of standards.

www.itgovernance.co.uk/shop/p-719.aspx

Information Security & ISO27001 Staff Awareness E-Learning

The most useful and complete online e-learning information security & ISO27001 staff awareness course available.

www.itgovernance.co.uk/shop/p-792.aspx

IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

IT Governance is your one-stop-shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT Governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/free_trial.aspx to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/free_trial.aspx for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting.aspx for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software.aspx for more information.

Contact us: + 44 (0) 845 070 1750

www.itgovernance.co.uk servicecentre@itgovernance.co.uk