

THE ISMS AND IT GOVERNANCE

What is an Information Security Management System?

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

ISO/IEC 17799:2005 is the international code of best practice for information security management – the statement of what should be in an ISMS, not how to design and manage it.

ISO/IEC 27001:2005 is a specification for the design of an ISMS – the how to make it work, not the details of what should be in it.

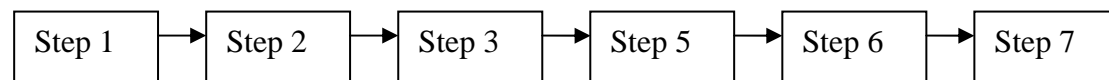
Information security is not just about anti-virus software, implementing the latest firewall or locking down your laptops or web servers. The overall approach to Information Security should be strategic as well as operational, and different security initiatives should be prioritised, integrated and cross-referenced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

An ISMS is also about ensuring that your systems comply with the requirements of critical regulations such as SOX, HIPAA, GLBA, State Breach Laws and others.

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 all international certification bodies. We have provided a representation (together with links to the appropriate ISO standards or IT Governance tools) of it below:



Step 1: Purchase and study a) the [Standards](#) and b) [Nine Steps to 7799 Success – an ISO27001 Implementation Overview](#)

Step 2: Assemble a team (including consultants if appropriate), agree project strategy, ISMS scope, purchase and read [International IT Governance: an Executive Guide to ISO27001/ISO17799](#), and draft an initial corporate information security policy.

Step 3: Asset inventory, risk assessment, & develop risk treatment plan – read [Information Security Risk Management for ISO 27001](#) and use a risk assessment tool such as [vsRisk](#).

Step 4: Draft statement of Applicability and supporting policies and procedures and get board approval– deploy an appropriate version of the [Complete ISMS Documentation Toolkit](#) to reduce the workload in this most labour-intensive part of the project

Step 5: Implement the ISMS, develop incident response procedures and provide training across the organization – *International IT Governance* provides guidance.

Step 6: Monitor, review, check and audit – ensuring that the ISMS works as planned – *International IT Governance* provides guidance.

Step 7: Identify and implement improvements prior to seeking (if appropriate) external certification – *International IT Governance* provides guidance.

THE ISMS AND IT GOVERNANCE

These steps fit within what is known as the Deming, or PDCA (for Plan-Do-Check-Act) cycle, which BS7799 requires to be applied in developing an ISMS.

How long does it take to implement an ISMS?

The answer to this question depends on many facts, including the size and complexity of the organization, the level of management commitment to the project, the underlying preparedness and current security posture of the organization, the level of expertise deployed in the project, and the organization's existing quality management culture.

Using traditional approaches, it's not uncommon for the whole project – from inception to completion of the first cycle of audits and reviews – to take from 14 to 19 months. And that's in an established, mid-size organization that is already reasonably secure. Using the IT Governance fast track approach, the total project time could be between four and seven months.

Challenges in creating the ISMS

Traditional approaches to implementing an ISMS are usually sequential. The company-wide 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. And 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.

There are 133 controls, each with a similarly complex set of challenges that have to be met before you can be sure that there will be no holes, no inconsistencies or incoherencies, in your ISMS.

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 FAST TRACK approach

You will want to tackle your project in one of two ways: either area by area (eg, 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.

Why use IT Governance Tools?

1. IT Governance books and toolkits are unique and fit for purpose – they are designed to give you the knowledge and information you need to cost-effectively implement an ISMS and accelerate organizational learning.
2. [International IT Governance](#) is the only book in the world that guides the project manager through every stage of the ISMS implementation process – and it's web-enabled, ensuring that you are able to access up-to-date

THE ISMS AND IT GOVERNANCE

information. Its quality is such that it is also the Open University's post graduate information security text book.

3. The [Complete ISMS Toolkit](#) is unique in its comprehensiveness, practical detail, updates and online drafting support – and it's consistent with, and follows the detailed guidance of, *International IT Governance*. It makes sense not to re-invent existing wheels when you can deploy pre-written policy and procedure templates.
4. Alan Calder sat for 7 years on the Certification Committee of a global certification body, Steve Watkins chairs a national ISMS chapter and the IT Governance team have experience of 7799 implementations dating from the earliest days of the standard. This expertise is now widely available through IT Governance books and tools.
5. IT Governance ISMS Toolkits are **fit for purpose**; custom kits, which include copies of the standards or of risk assessment tools, exist to help you save money when you set out to tackle ISO27001. You can see the full range of kits: www.27001.com/ISMSFreeDemo.aspx

[Complete ISMS Documentation Toolkit](#)

For less than one day of a consultant's time, our **Complete Toolkit** gives you:

- A model, pre-written Information Security Policy, Statement of Applicability and Information Security Manual (approximately 50 pages)
- An encapsulation of all the detailed ISMS knowledge and experience of the IT Governance consultancy team – focused on *YOUR* ISMS requirements
- Approximately 110 different pre-written documents, totalling nearly 400 pages
- No software to install – easy-to-use toolkit on standard MS Word
- Our unique documentation support service, giving you guidance on issues of adaptation, customisation and understanding, as and when they arise, simplifying and supporting your progress throughout the project
- Our 12 month automatic update service ensures that you automatically benefit from planned improvements to the toolkit.
- “The **ISMS Documentation Toolkit** is a unique blend of an outstanding, practical and comprehensive suite of pre-written document templates and value adding services that will **save you months of work** and get your ISMS project off to a flying start. “ Alan Calder, author of “[IT Governance: a Manager's Guide to Information Security and BS7799/ISO17799](#)”.

THE ISMS AND IT GOVERNANCE

BENEFITS OF THE *ISMS DOCUMENTATION TOOLKIT*:

- Accelerates your ISMS project
- Reduces your project (internal resource and external support) costs
- Cost-effectively deploys best practice
- Makes you your own expert
- Gives you online access to drafting expertise
- Ensures that all the ISMS control areas and controls are comprehensively and professionally addressed
- Ensures alignment and consistency between procedures and work instructions across the whole ISMS
- Avoids costly, credibility-destroying trial-and-error methods
- Accelerates organizational learning
- Crystallizes your approach to complex issues
- Catalyses how you deal with specific threats and controls
- Brings continual improvements to ensure your ISMS stays ahead of the security threat curve
- Pre-written model policies and processes account for all the key issues
- Templated forms and documents save you time
- Integrates with the practical, detailed advice in "[*International IT Governance: an Executive Guide to ISO27001/ISO17799*](#)".

"IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799"

"This book provides a comprehensive guide as to actions that should be taken." NIGEL TURNBULL, Chairman, Lasmo Plc, author of the Turnbull Report.

"...underpins professional practice in InfoSec Management. Following the standard, risk management guidance is given for each InfoSec area, including the trade-offs that arise between covering a vulnerability and leaving it uncovered. For complete coverage of the standard, this is unparalleled, and that's why we have chosen it as the basis for the Open University's new Information Security Management Course." Dr Jon G Hall, Lecturer in Information Security, Open University, UK.

"...essential....for anyone involved in preparing for and maintaining BS7799 certification within their organisation. It is not only essential reading, but also a critical source when preparing and managing the ISMS. We used it extensively as a key reference during our BS7799 certification activities over the past two years. Without this source of practical advice the task would have been significantly harder." Bill Pepper
Director of Security Risk Management CSC

"....a clear and authoritative guide to this important standard. It gives a through coverage of the requirements of the standard and practical guidance on what actions to take to achieve compliance..." Roger Pawling, Countryside Council for Wales