BEST PRACTICE

A MANAGEMENT GUIDE

Implementing Information Security

based on ISO 27001 / ISO 27002

Implementing Information Security based on ISO 27001/ISO 27002 -
A Management Guide

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT management
- Architecture (Enterprise and IT)
- Business management and
- Project management

Van Haren Publishing offers a wide collection of whitepapers, templates, free e-books, trainer material etc. in the **VHP Knowledge Base**: www.vanharen.net for more details.

VHP is also publisher on behalf of leading organizations and companies:
ASLBiSL Foundation, CA, Centre Henri Tudor, Gaming Works, Getronics, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, Quint, The Open Group, The Sox Institute, Tmforum.

Topics are (per domain):

IT (Service) Management / IT Governance
ABC of ICT
ASL
BiSL
CATS CM®
CMMI
CoBIT
Frameworx
ISO 17799
ISO 27001
ISO 27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL®
ITSM
MOF
MSF
SABSA

Architecture (Enterprise and IT)
Archimate®
GEA®
SOA
TOGAF®

Business Management
Contract Management
EFQM
eSCM
ISA-95
ISO 9000
ISO 9001:2000
OPBOK
Outsourcing
SAP
SixSigma
SOX
SqEME®

Project/Programme/ Risk Management
A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP™
P3O®
PMBOK® Guide
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Implementing Information Security based on ISO 27001/ISO 27002

A Management Guide

Colophon

Title:	Implementing Information Security based on ISO 27001/ISO 27002 - A Management Guide
Series:	Best Practice
Lead Author:	Alan Calder
Chief Editor:	Jan van Bon
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 541 4
Print:	First edition, first impression, May 2006 First edition, second impression, November 2007 First edition, third impression, January 2009 Second edition, first impression, July 2009 Second edition, second impression, September 2011
Design and Layout:	CO2 Premedia, Amersfoort – NL
Copyright:	© Van Haren Publishing 2009

This title was updated in 2009 to reflect changes made to the Standard in 2008.

Permission to reproduce extracts of BS ISO/IEC 27001: 2005 (BS 7799-2: 2005) is granted by BSI. British Standards can be obtained from BSI Customer Services, 389 Chiswick High Road, London W4 4AL. Tel: +44 (0)20 8996 9001.
email: cservices@bsi-global.com

For any further enquiries about Van Haren Publishing, please send an e-mail to:
info@vanharen.net

Aknowledgements

Van Haren Publishing would like to thank Alan Calder, the lead author, for his expert, flexible approach and his professional delivery.

Title: Implementing Information Security based on ISO 27001/ ISO 27002
A Management Guide

Lead Author: Alan Calder

Editors: Jan van Bon (Inform-IT), Chief Editor
Selma Polter, Editor

Review Team: Dr Gary Hinson — IsecT
Steve G Watkins, — HMCPSI (UK Government: Crown Prosecution Service Inspectorate)
Dr Jon G. Hall — Centre for Research in Computing, The Open University

Contents

CHAPTER 1

Introduction

This Management Guide provides an overview of the implementation of an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2005 and which uses controls derived from ISO/IEC 27002:2005.
This book is intended as a companion to the *Management Guide on ISO 27001& ISO 27002*, so it repeats very little of that book's information about the background and components of the two information security standards. It is an overview of implementation, rather than a detailed implementation guide, and it is not a substitute for reading and studying the two Standards themselves.

1.1 ISO/IEC 27001:2005 ('ISO 27001' or 'the Standard')

This is the most recent, most up-to-date, international version of a standard specification for an Information Security Management System. It is vendor-neutral and technology-independent. It is designed for use in organizations of all sizes ('intended to be applicable to all organizations, regardless of type, size and nature'[1]) and in every sector (e.g. 'commercial enterprises, government agencies, not-for-profit organizations'[2]), anywhere in the world. It is a management system, not a technology specification and this is reflected in its formal title, which is "Information Technology - Security Techniques - Information Security Management Systems - Requirements." ISO 27001 is also the first of a series of international information security standards, all of which will have ISO 27000 numbers.

1.2 ISO/IEC 27002:2005 ('ISO 27002')

This Standard is titled "Information Technology - Security Techniques - Code of Practice for information security management." Published in July 2005, it replaced ISO/IEC 17799:2000, which has now been withdrawn. This Standard now has the number ISO/IEC 27002, in order to clarify that it belongs to the ISO/IEC 27000 family of standards.

1.3 Definitions

ISO 27001 defines an ISMS, or Information Security Management System, as 'that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.'
Other definitions are intended to be consistent with those used in related information security standards, such as ISO/IEC 27006:2005, ISO/IEC 27005:2007 et cetera.
An ISMS needs a consistent set of definitions, so that there is a consistent understanding of its requirements across all those who are within its scope. The definitions of ISO 27001 should be adopted, supported where necessary by additional definitions from ISO 27002.

1) ISO/IEC 27001:2005 Application 1.2
2) ISO/IEC 27001:2005 Scope 1.1

CHAPTER 2

Information security and ISO 27001

Effective information security is defined in the Standard as the 'preservation of confidentiality, integrity and availability of information.'[3] It cannot be achieved through technological means alone, and should never be implemented in a way that is either out of line with the organization's approach to risk or which undermines or creates difficulties for its business operations.

2.1 Approach to information security

The ISMS includes 'organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources'[4] and is a structured, coherent management approach to information security. It should be designed to ensure the effective interaction of the three key attributes of information security:

- process (or procedure);
- technology;
- behavior.

The decision to develop an ISMS should be a strategic business decision. It should be debated, agreed and driven by the organization's board of directors or equivalent top management group. The design and implementation of the ISMS should be directly influenced by the organization's 'needs and objectives, security requirements, the processes employed and the size and structure of the organization.'[5]

2.2 The ISMS and organizational needs

ISO 27001 is not a one-size-fits-all solution to an organization's information security management needs. It should not interfere with the growth and development of the business. According to ISO 27001:

3) ISO/IEC 27001:2005 Terms and Definitions 3.4
4) ISO/IEC 27001:2005 Terms and Definitions 3.7 Note
5) ISO/IEC 27001:2005 Introduction General 0.1

- the ISMS 'will be scaled in accordance with the needs of the organization'
- a 'simple situation requires a simple ISMS solution';
- the ISMS is 'expected to change over time';
- the Standard is meant to be a useful model for 'establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS.'[6]

It is a model that can be applied anywhere in the world, and understood anywhere in the world. It is also technology-neutral and can be implemented in any hardware or software environment.

2.3 Reasons to implement an ISMS

There are, broadly, four reasons for an organization to implement an ISMS:

- *strategic* - a government or parent company requirement, or a strategic board decision, to better manage its information security within the context of its overall business risks;
- *customer confidence* - the need to demonstrate to one or more customers that the organization complies with information security management best practice, or the opportunity to gain a competitive edge, in customer and supplier relationships, over its competitors;
- *regulatory* - the desire to meet various statutory and regulatory requirements, particularly around computer misuse, data protection and personal privacy;
- *internal effectiveness* - the desire to manage information more effectively within the organization.

While all four of these reasons for adopting an ISMS are good ones, it must be remembered that having an ISO 27001-compliant ISMS will not automatically 'in itself' confer immunity from legal obligations.' The organization will have to ensure that it understands the range of legislation and regulation with which it must comply, ensure that these requirements are reflected in the ISMS as it is developed and implemented, and then ensure that the ISMS works as designed.

As figure 2.1 illustrates, an ISMS potentially enables an organization to deliver against all four of these objectives.

---

6) All 4 quotes from ISO/IEC 27001:2005 Introduction General 0.1

7) ISO/IEC 27001:2005 Title Note

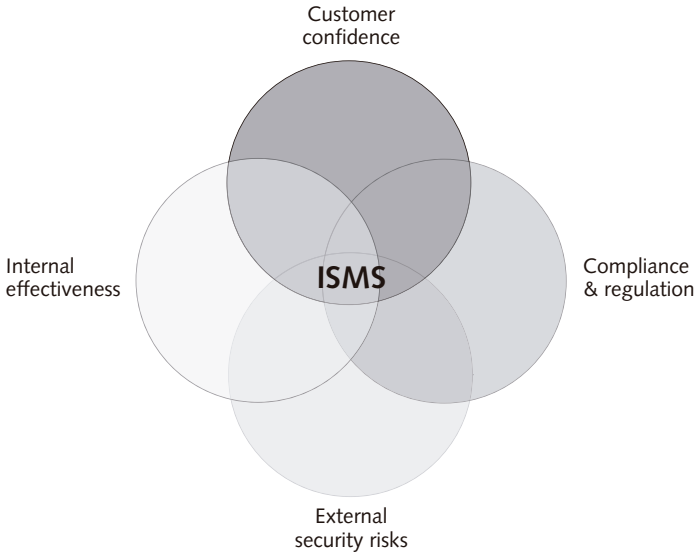

Figure 2.1 *Strategic information risk management*

2.4 The ISMS and regulation

Regulations and the law in each of the areas mentioned above are still evolving; they are sometimes poorly drafted, often contradictory (particularly between jurisdictions) and have little or no case law to provide guidance for organizations in planning their compliance efforts. It can be difficult for organizations to identify specific methods for complying with individual laws. In these circumstances, implementation of a best practice ISMS may, in legal proceedings, support a defense in court that the management did everything that was reasonably practicable for it to do in meeting its legal and regulatory requirements. Of course, every organization would have to take its own legal advice on issues such as this and neither this book nor this author provides guidance of any sort on this issue.

As figure 2.2 demonstrates, an ISMS enables an organization to meet existing, clearly defined regulatory compliance requirements as well as those that are still emergent and are either unclear or untested.

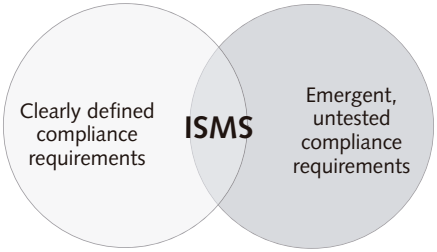

Figure 2.2 *The ISMS and regulation*

CHAPTER 3

Certification

ISO/IEC 27001:2005 is a specification for an ISMS. It is not a set of guidelines or a Code of Practice. Any organization that implements an ISMS which it wishes to have assessed against the Standard will have to follow the specification contained in the Standard. As a general rule, organizations implementing an ISMS based on ISO/IEC 27001:2005 will need to pay close attention to the wording of the Standard itself, and to be aware of any revisions to it. Non-compliance with any official revisions, which usually occur on a three-year and a five-year cycle, will jeopardize an existing certification.

3.1 Read and study the Standards

The Standard itself is what an ISMS will be assessed against; where there is any conflict between advice provided in this or any other guide to implementation of ISO 27001 and the Standard itself, it is the wording in the Standard that should be heeded. An external certification auditor will be assessing the ISMS against the published Standard, not against the advice provided by this book, a sector scheme manager, a consultant or any other third party. It is critical that those responsible for the ISMS should be able to refer explicitly to its clauses and intent and be able to defend any implementation steps they have taken against the Standard itself.

An appropriate first step is to obtain and read copies of ISO/IEC 27001:2005 and ISO/IEC 27002:2005. Copies can be purchased from the ISO website, from national standards bodies and from www.itgovernance.co.uk; standards should be available in hard copy and downloadable versions.

ISO 27001 provides a specification against which an organization's ISMS can be independently audited by an accredited certification body. If the ISMS is found to conform to the specification, the organization can be issued with a formal certificate confirming this.

3.2 'Badge on the wall' debate

There are two approaches to implementation of the Standard:

- develop and implement an ISMS to meet the requirements of the Standard and have it certificated;
- develop and implement an ISMS but do not seek certification.

This is known as 'the badge on the wall' debate.

The argument in favor of certification is, in essence, that this route enables other organizations (customers, partners and suppliers) to obtain, without having to carry out their own audit, a level of reassurance about the effectiveness and completeness of the ISMS. It can also be presented as evidence of compliance with many aspects of information-related regulation.

The argument against is that a 'badge on the wall' is not necessary to prove to the organization that its ISMS is adequate or that it is doing a good job of preserving information security.

ISO 27001 is drafted, as is all guidance on implementation, on the assumption that the organization implementing an ISMS ISO 27001 will seek certification; ISO 27002 provides guidance for organizations that simply wish to develop an ISMS that uses best practice controls. Any organization that claims it has an ISO 27001-compliant ISMS but which has not subjected itself to certification should, under the risk assessment requirements of the Standard, be treated like any other organization that *does not have an adequate information security management system* - until proven otherwise.

Four broad reasons were identified, in the previous chapter, for implementing an ISO 27001-conforming ISMS. While two of them (customer confidence and regulatory best practice demonstration) can only be achieved through certification, the other two could perhaps be achieved without.

However, as most people recognize, independent third party verification has a reliable track record in helping organizations make a success of almost any initiative.

Third party certification is an absolute necessity for any ISO 27001 ISMS; not only does it give management and the business an initial, as well as an ongoing, target at which to aim, but it also ensures that the Standard is properly understood and effectively implemented.

3.3 Certification

The *Management Guide to ISO27001 & ISO27002* provides an overview of the certification process and the Standards under which accredited certification auditors are required to operate.

3.4 Qualifications and further study

It is an expectation of ISO 27001 that its implementation will be in the hands of qualified people. Appropriate qualifications can be obtained in a number of ways, included through the UK Open University's information Security course and the British Computer Society's ISEB information security qualification. In addition, many certification bodies offer ISO 27001 lead auditor training courses.
Practitioners should also keep themselves up-to-date with current developments within the information security field, both through industry journals and magazines, and through relevant industry websites, such as www.itgovernance.co.uk/iso27001.aspx.

CHAPTER 4

ISO 27001 and ISO 27002

It is important to understand the relationship between the two information security Standards.

4.1 ISO 27002

ISO/IEC 27002:2005 is a **Code of Practice**. It provides **guidance** and uses words like '*may*' and '*should*'. It provides an internationally accepted framework for best practice in Information Security Management and systems interoperability. It also provides guidance on how to implement an ISMS capable of certification, to which an external auditor could refer. It does not provide the basis for an international certification scheme.

4.2 ISO 27001

ISO/IEC 27001:2005 is a **specification** for an ISMS. It sets out **requirements** and uses words like '*must*' and '*shall*'. One mandatory requirement is that 'control objectives and controls from Annex A shall be selected' in order to meet the 'requirements identified by the risk assessment and risk treatment process.'[8] Annex A to ISO/IEC 27001:2005 lists the 133 controls that are in ISO/IEC 27002:2005, follows the same numbering system as that Standard and uses the same words and definitions.

As the preface to ISO 27001 states, 'the control objectives and controls referred to in this edition are directly derived from and aligned with those listed in ISO/IEC 27002:2005.'[9] ISO 27002, though, provides substantial implementation guidance on how individual controls should be approached. Anyone implementing an ISO 27001 ISMS will need to acquire and study copies of both ISO 27001 and ISO 27002.

While ISO 27001 in effect mandates the use of ISO 27002 as a source of guidance on controls, control selection and control implementation, it does not limit the organization's choice of controls to those in ISO 27002. The preface goes on to state: 'The list of control objectives and controls in this ISO Standard is not exhaustive and an organization might consider that additional control objectives and controls are necessary.'[10]

8) ISO/IEC 27001:2005 4.2.1 g) Select control objectives and controls for the treatment of risks

9) ISO/IEC 27001:2005 Preface

10) Ibid.

CHAPTER 5

Frameworks and management system integration

ISO 27001 is designed to harmonise with ISO 9001:2008 and ISO 14001:2004. This makes it possible to develop a completely integrated management system that can achieve certification to ISO 27001, ISO 9001 and ISO 14001.

'It is essential that your ISMS is fully integrated into your organization; it will not work effectively if is a separate management system and exists outside of and parallel to any other management systems. Logically, this means that the framework, processes and controls of the ISMS must, to the greatest extent possible, be integrated with, for instance, your ISO 9001 quality system; you want one document control system, you want one set of processes for each part of the organization, etc. Clearly, therefore, assessment of your management systems must also be integrated: you only want one audit, which deals with all the aspects of your management system. It is simply too disruptive of the organization, too costly and too destructive of good business practice, to do anything else.'[11]

There are significant cost benefits to be obtained from this sort of streamlining; these come in addition to the significantly more important benefits that are derived from improving the focus and cohesiveness of the organization's quality assurance activities.

5.1 ITIL

ITIL (the IT Infrastructure Library) is a set of best practices at the heart of IT service management. The most recent version is ITILv3, the IT Lifecycle Management Process. ITILv2 includes one manual titled 'Best Practice for Security Management', which was written and published in 1999. This manual aligns with **BS7799:1995**, although it also took BS7799:1999 (draft) into account. This means that it was written before the publication of BS7799 as a two-part standard and is aligned with what is now ISO 17799, although the version with which it is aligned has now been updated twice.

The manual's starting point is existing ITIL processes, to which it then adds security processes. Although it is technically out-of-date, it still supplies extremely useful guidance to any organization that treats any part of its IT operation as a 'service', particularly if that service is the subject of an SLA, whether internal or external.

11) IT Governance: a Manager's Guide to Data Security and ISO27001/ISO27002 (4th edition), Alan Calder and Steve Watkins, published by Kogan Page 2008, page 338

5.2 ISO 20000

ISO/IEC 20000-1 is the Standard that specifies best practice for IT service management, and is the specification for IT service management against which an organization's actual practices can be certified.
Clause 6.6 of ISO 20000-1 deals with information security. It cross-refers to ISO 27002. It requires:

- management to approve an information security policy
- communicating it to all relevant personnel and customers;
- selecting security controls on the basis of a risk assessment;
- implementing and operating appropriate security controls;
- including security in third party agreements;
- implementing an information security incident management procedure;
- measuring and monitoring information security activities;
- planning to improve information security.

Clearly, these requirements are best met by implementing an information security management system that conforms to ISO 27001.
Any organization that is pursuing ISO 20000 should think through, before project initiation, how it will integrate these two management systems. There is already some commonality between the two and, while information security is treated as an important aspect of IT service management, IT service management is also treated as an important area in information security.

5.3 ISO 27001 Annex C

Annex C to ISO 27001 (which is informative, not mandatory - no organization is required to try and integrate its management systems) shows how its individual clauses correspond to the clauses of ISO 9001:2008 and ISO 14001:2004.

While Annex C includes the correspondence with ISO 14001:2004, table 5.1 shows instead the correspondences between ISO 27001, ISO 9001 and ISO 20000-1:2005.

ISO 27001:2005	ISO 9001:2008	ISO 20000-1:2005
4 Information Security Management System	4 Quality Management System	3 Requirements for a management system
4.1 General requirements		4 Planning and implementing service management
4.2 Establishing and managing the ISMS	4.1 General requirements	
4.2.1 Establish the ISMS		4.1 Plan service management
4.2.2 Implement & operate the ISMS		
		4.2 Implement service management and provide the services
4.2.3 Monitor and review the ISMS	8.2.3 Monitoring and measurement of processes	4.3 Monitoring, measuring and reviewing
	8.2.4 Monitoring and measurement of product	
4.2.4 Maintain & improve the ISMS		4.4 Continual improvement
		3.2 Documentation
4.3 Documentation requirements	4.2 Documentation requirements	requirements
4.3.1 General	4.2.1 General	
	4.2.2 Quality manual	
4.3.2 Control of documents	4.2. Control of documents	
4.3.3 Control of records	4.2.4 Control of records	
5 Management responsibility	5 Management responsibility	3.1 Management responsibility
5.1 Management commitment	5.1 Management commitment	
	5.2 Customer focus	4.4.1 Policy
	5.3 Quality policy	
	5.4 Planning	
	5.5 Responsibility, authority and communication	
5.2 Resource management	6 Resource management	
5.2.1 Provision of resources	6.1 Provision of resources	
	6.2 Human resources	
5.2.2 Training, awareness and competence	6.2.2 Competence, awareness and training	3.3 Competence, awareness and training
	6.3 Infrastructure	
	6.4 Work environment	
6 Internal ISMS audits	8.2.2 Internal audit	Included in 4.3
7 Management review of the ISMS	5.6 Management review	
	5.6.1 General	
7.1 General	5.6.2 Review input	
7.2 Review input	5.6.3 Review output	
7.3 Review output		
8 ISMS improvement	8.5 Improvement	4.4.2 Management of improvements
8.1 Continual improvement	8.5.1 Continual improvement	
8.2 Corrective action		
8.3 Preventive action	8.5.2 Corrective action	
	8.5.3 Preventive action	

Table 5.1 *Correspondences between ISO 27001, ISO 9001 and ISO 20000-1:2005*

5.4 Management system integration

For many organizations, the critical correspondences will be between ISO 27001 and ISO 9001 and it is in the areas of obvious overlap that the integration of management systems starts. Practically speaking, the most important overlaps are:

- Clause 4.3, which deals with documentation requirements;
- Clause 5.1, which deals with management commitment;
- Clause 7, which deals with management review;
- Clause 8, which deals with management system improvement;
- Clause 6, which deals with internal audits.

What these clauses make possible between them is the deployment of common documentation, management and audit processes for both management systems. For instance, the organization only needs a single management system that incorporates its quality and its information security procedures, a single comprehensive and integrated audit process that covers all aspects of its activity, and a standard management authorization, approval, monitoring, review and quality improvement process that deals with all its activities irrespective of whether they fall within the scope of the information security management system, the quality management system or the environmental management system.

The note to Clause 1.2 of ISO 27001 recognizes this simple principle: 'If an organization already has an operative business process management system, it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system.'

5.5 BS25999

BS25999 provides a specification for a business continuity framework that can make a significant contribution to the development of the business continuity plan(s) that are specified as being required in Clause A. 14 of the Annex to ISO 27001 (for medium and large organizations and often for smaller ones). ISO 27001 pre-supposes the existence of a business continuity plan.

The only formal standard to which organizations can turn is BS25999. It makes practical sense for an organization to seek guidance on such a mission-critical subject from a standard such as this. Copies of BS25999 can be obtained from BSI and from other standards distributors.

BS25999 uses terms that will be familiar to those developing an ISMS, including 'risk assessment' and 'impacts'. The principle that ought to be applied is that, where there

is any gap between the requirements of ISO 27001 (including in definitions, process, etc) and the guidance of BS25999, it is ISO 27001 that must have primacy. A business continuity framework developed in line with BS25999 will certainly be adequate to the requirements of an information security management system and will be capable of supporting the information security control requirements of ISO 27001's Clause A.14.

5.6 CobiT

CobiT, or Control Objectives for Information and related Technology (now in version 4.1), is 'a model for the control of the IT environment.'[13] While this book is not about CobiT, anyone deploying an ISO 27001 ISMS should be aware of it. The *Management Guide to ISO 27001& ISO 27002* includes a chapter on the relationship between ISO 27001 and CobiT.

The key areas of correspondence between ISO 27001 and CobiT are shown in table 5.2.

ISO 27001		**CobiT 4.1**	
4.2.1.a & b	Define ISMS scope and policy	PO6	Communicate management aims and direction
4.2.1.c et seq	Risk assessment	PO9	Assess and manage IT risks
4.2.2.e and 5.2.2.	Training and awareness	DS7	Educate and train users
4.2.2.f	Manage operations	DS13	Manage operations
4.2.2.h & 8	Security incidents and continuous improvement	DS10	Manage problems and incidents
4.2.3	Monitor and review	ME1	Monitor & evaluate IT performance & ME2 Monitor & evaluate internal control
4.3	Documentation requirements	PO4	Define the IT processes
6	Internal ISMS audits	ME2	Monitor & evaluate internal control

Table 5.2 *Key areas of correspondence between ISO 27001 and CobiT*

13) IT Governance based on CobiT: A Management Guide, Van Haren Publishing 2004, page 23