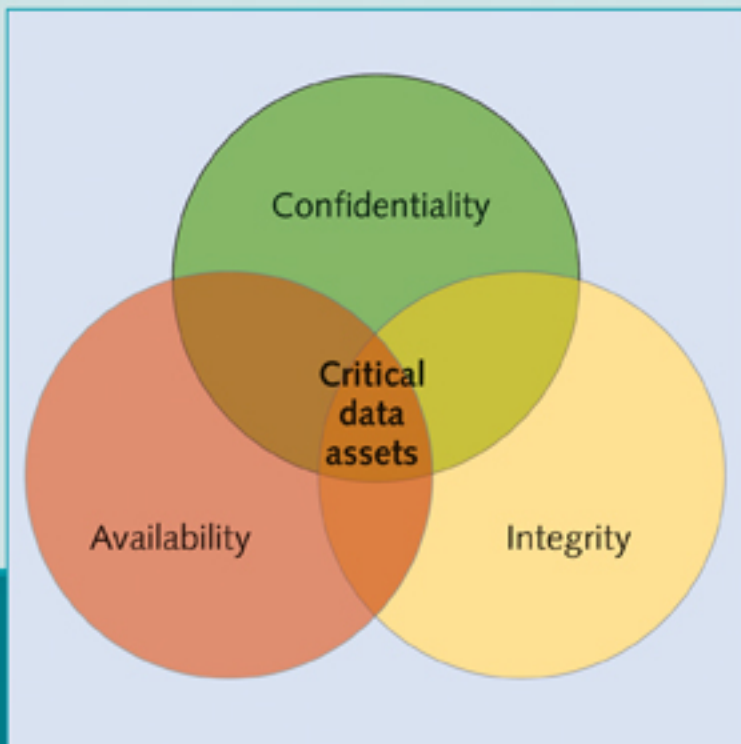


A MANAGEMENT GUIDE

Information Security

based on ISO 27001 / ISO 27002



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

These publications are grouped in series: *ITSM Library*, *Best Practice* and *IT Management Topics*. VHP is also publisher on behalf of leading companies and institutions:

The Open Group, IPMA-NL, PMI-NL, CA, Getronics, Quint, The Sox Institute and ASL BiSL Foundation

Topics are (per domain):

IT (Service) Management / IT Governance

ASL
BiSL
CATS
CMMI
COBIT
ISO 17799
ISO 27001
ISO/IEC 20000
ISPL
IT Service CMM
ITIL® V2
ITIL® V3
ITSM
MOF
MSF
ABC of ICT

Architecture (Enterprise and IT)

Archimate®
GEA®
TOGAF™

Business Management
EFQM
ISA-95
ISO 9000
ISO 9001:2000
SixSigma
SOX
SqEME®

Project/Programme/ Risk Management

A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP
PMBok®
PRINCE2®

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

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



Colophon

Title:	Information Security based on ISO 27001 / ISO 27002 - A Management Guide
Series:	Best Practice
Author:	Alan Calder
Chief Editor:	Jan van Bon
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 540 7
Edition:	First edition, first impression, May 2006 First edition, second impression, May 2008 Second edition, first impression, July 2009
Design and layout:	CO2 Premedia, Amersfoort-NL
Copyright:	© Van Haren Publishing, 2006, 2009
Printer:	Wilco, Amersfoort - NL

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

Although this publication has been composed with most care, neither author nor editor, nor publisher can accept any liability for damage caused by possible errors and/or incompleteness in this publication.

No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by the publisher.

Aknowledgements

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

Title: 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

1	Introduction	1
1.1	Originating body: ISO/IEC JTC1/SC 27	1
1.2	ISO/IEC 27001:2005 ('ISO 27001' or 'the Standard')	1
1.3	ISO/IEC 27002:2005 ('ISO 27002')	2
1.4	Definitions	2
2	Information security	3
2.1	Risks to information assets	3
2.2	Information security	4
2.3	Information Security Management System	4
3	Background to the Standards	5
3.1	First certification	5
3.2	ISO 17799:2000	5
3.3	BS7799-2	6
3.4	International adoption	6
3.5	Translations and sector schemes	7
3.6	ISO 27001:2005	7
4	Relationship between the Standards	9
4.1	Why develop an international code of practice?	9
4.2	Correspondence between the two Standards	10
5	Use of the Standards	11
5.1	Specification compared to a Code of Practice	11
5.2	The ISMS	12
5.3	ISO 27001 as a model for the ISMS	12
6	Certification process and certification bodies	13
6.1	Certification bodies	13
6.2	Standards for certification bodies	13
6.3	The certification process	14
6.4	The formal audit	15
6.5	The audit report	15
6.6	Outcome of the audit	15
7	Overview of ISO 27001	17
7.1	Main clauses	17

7.2	ISMS building blocks: relationship between ISO/IEC 27001 Clauses 4-8, ISO/IEC 27001 Annex A, and ISO/IEC 27002	18
7.3	General requirements	19
7.4	Other content	20
8	Summary of changes from BS7799-2:2002.....	21
8.1	Greater clarity in specifications	21
9	Overview of ISO 27002:2005	23
9.1	The security categories	24
9.2	ISMS building blocks: relationship between the control clauses of ISO/IEC 27002:2005.....	24
10	Summary of changes from ISO 27002:2000	27
10.1	Clause changes.....	27
10.2	Layout of controls	27
10.3	Control changes.....	28
11	ISO 27000 series in future	29
11.1	ISO 27001	29
11.2	ISO 27002	29
11.3	ISO 27003	29
11.4	ISO 27004	29
11.5	ISO/IEC 27005:2008	30
12	Compatibility and integration with other management systems	31
12.1	ISO 27001 Annex C and integration	31
12.2	The integrated management system.....	31
12.3	ISO 9001	32
12.4	BS25999	32
13	Documentation requirements and record control	33
13.1	Document control requirements.....	33
13.2	Contents of the ISMS documentation.....	34
13.3	Record control	35
13.4	Annex A document controls.....	35
14	Management responsibility.....	37
14.1	Management direction.....	37
14.2	Providing evidence of management commitment	37
14.3	Management-related controls.....	38
14.4	Requirement for management review.....	39

15	Process approach and the PDCA cycle.....	41
15.1	PDCA and ISO 27001.....	41
15.2	PDCA applied at the tactical level	42
15.3	PDCA cycle linked to the clauses of ISO 27001	42
16	Scope definition	45
16.1	The scoping exercise	45
16.2	Small organizations.....	45
16.3	Larger organizations.....	46
16.4	Legal and regulatory framework.....	46
17	Policy definition.....	47
17.1	Policy and business objectives	47
17.2	Information security governance and the ISMS.....	48
18	Risk assessment	49
18.1	Links to other standards	49
18.2	Objectives of risk treatment plans.....	49
18.3	Risk assessment process.....	50
18.4	Assets within the scope (4.2.1.d1).....	50
18.5	Asset owners	51
18.6	Threats (4.2.1.d2)	51
18.7	Vulnerabilities (4.2.1.d3).....	52
18.8	Impacts (4.2.1.d4).....	52
18.9	Risk assessment (4.2.1.e).....	52
18.10	Likelihood.....	53
18.11	Calculate the risk level	53
19	Risk treatment plan.....	55
19.1	Documenting the risk treatment plan	55
19.2	Risk treatment plan and PDCA approach	56
20	The Statement of Applicability	57
20.1	Controls and Annex A	57
20.2	Controls (4.2.1.f.1)	57
20.3	Residual risks	58
20.4	Control objectives.....	58
20.5	Plan for security incidents.....	58
21	Do - implement and operate the ISMS.....	61
21.1	Implementation	61

22	Check - monitor and review the ISMS	63
22.1	Monitoring.....	63
22.2	Auditing	63
22.3	Reviewing	64
23	Act - maintain and improve the ISMS	65
23.1	Management review	65
24	ISO 27001:2005 Annex A	67
24.1	SoA and external parties.....	67
24.2	Annex A clauses	67
25	Annex A control areas and controls.....	69
25.1	Clause A5: Security policy	69
25.2	Clause A6: Organization of information security	69
25.3	Clause A7: Asset management	70
25.4	Clause A8: Human resources security	70
25.5	Clause A9: Physical and environmental security	71
25.6	Clause A10: Communications and operations management.....	71
25.7	Clause A11: Access control.....	73
25.8	Clause A12: Information systems acquisition, development and maintenance.....	74
25.9	Clause A13: Information security incident management.....	75
25.10	Clause A14: Business continuity management.....	75
25.11	Clause A15: Compliance.....	76
26	ISO 27001 and CobiT	77
26.1	Background to CobiT.....	77
26.2	CobiT framework.....	77
26.3	CobiT process DS5	78
26.4	Gaps and overlaps	78
27	ISO 27001, ITIL and ISO 20000.....	81
27.1	ITIL	81
27.2	Background to ITIL	81
27.3	BS15000/ISO 20000	82
27.4	ITIL Security Management	82
27.5	ISO 27001, ITIL and CobiT	82
A	Bibliography of related standards and guides	83
B	Accredited certification and other bodies.....	85

Introduction

This Management Guide provides an overview of the two international information security standards, ISO/IEC 27001:2005 and ISO/IEC 27002:2005.

It provides an introduction and overview to both the Standards. It is not a substitute for acquiring (from national standards bodies or licensed online resellers) and reading the Standards themselves. This book briefly describes the background to the current version of the Standards. It also looks briefly at links to other standards, such as *ISO 9001*, *BS25999* and *ISO 20000*, and to frameworks such as *CobiT* and *ITIL*. Above all, it describes how ISO 27001 and ISO 27002 interact to guide organizations in the development of best practice information security management systems.

1.1 Originating body: ISO/IEC JTC1/SC 27

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) have established a joint technical committee, ISO/IEC JTC 1, to deal with their mutual interest in the field of information technology. This committee has a number of sub-committees; one of these, SC 27, is responsible for IT security techniques. This committee is responsible for producing both the Standards described in this Management Guide.

1.2 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.

1.3 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. While it was initially numbered ISO/IEC 17799, this standard has also been given the number ISO/IEC 27002 number in order to make it a member of the ISO27000 series of standards.

1.4 Definitions

The definitions used in both Standards are intended to be consistent with one another and also to be consistent with those used in related information security standards, such as ISO/IEC Guide 73:2002, ISO/IEC 13335-1:2004, etc.

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

Information security

It is a truism to say that information is the currency of the information age. Information is, in many cases, the most valuable asset possessed by an organization, even if that information has not been subject to a formal and comprehensive valuation.

IT governance is the discipline that deals with the structures, standards and processes that boards and management teams apply to effectively manage, protect and exploit their organization's information assets.

Information security management is that subset of IT governance that focuses on protecting and securing an organization's information assets.

2.1 Risks to information assets

An asset is defined in ISO 27001 as 'anything that has value to an organization'. Information assets are subject to a wide range of threats, both external and internal, ranging from the random to the highly specific. Risks include acts of nature, fraud and other criminal activity, user error and system failure. Information risks can affect one or more of the three fundamental attributes of an information asset: its:

- availability;
- confidentiality;
- integrity.

These three attributes are defined in ISO 27001 as follows:

- *availability* - 'the property of being accessible and usable upon demand by an authorized entity', which allows for the possibility that information has to be accessed by software programs as well as human users;
- *confidentiality* - 'the property that information is not made available or disclosed to unauthorized individuals, entities, or processes';
- *integrity* - 'the property of safeguarding the accuracy and completeness of assets'.

2.2 Information security

ISO 27001 defines information security as the ‘preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.’

2.3 Information Security Management System

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.’ An ISMS exists to preserve confidentiality, integrity and availability. As figure 2.1 shows, the ISMS secures the confidentiality, availability and integrity of the organization’s information and information assets, and its most critical information assets are those for which all three attributes are important.

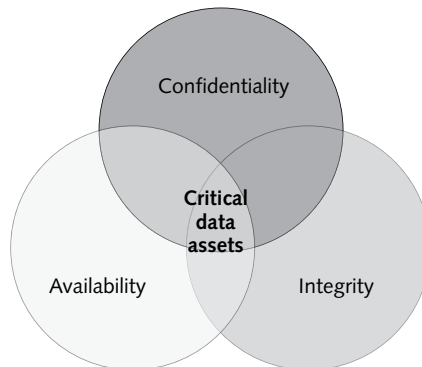


Figure 2.1 Attributes of Information Assets

Background to the Standards

The information security standard, BS7799, was first issued in April 1999, as a two-part standard. An earlier Code of Practice had been substantially revised and became Part 1 of the new standard (BS7799-1:1999) and a new Part 2 (BS7799-2:1999) was drafted and added.

Part 1 was titled 'Code of Practice for Information Security Management' and it provided guidance on best practice in information security management. Its foreword clearly stated that it was not to be treated as a specification.

Part 2, titled 'Specification for Information Security Management Systems,' was drafted as the specification against which an organization's security management system could be assessed and certificated.

The link between the two Standards was, from the outset, through Annex A of BS7799-2, which lists all the information security controls whose applicability organizations are required to consider. This list of controls is aligned with the controls of BS7799-1, and BS7799-2 requires the user to seek more detailed guidance on how to implement the listed controls from BS7799-1.

3.1 First certification

The first organization in the world to have its ISMS certified as being in conformance with BS7799-2:1999 was Business Link London City Partners. Since then, there have been nearly two thousand certifications; by December 2008, there were over 7,000 certifications.

3.2 ISO 17799:2000

BS7799-1:1999 began to be adopted by other national standards bodies becoming, for instance, AS 4444 in Australia and NZS 4444 in New Zealand. The International Standards Organization (ISO) and the International Electrotechnical Commission

(IEC)³ then collaborated to adopt and internationalize BS7799-1 as ISO/IEC 17799:2000 in December 2000.

This version of the Guidelines was dual numbered in some countries so that, for example, in the UK it was numbered BS7799-1:2000 (ISO/IEC 17799:2000). It was exactly the same document, whatever number it was given.

ISO 17799 was substantially revised, improved and updated five years later and, as ISO/IEC 17799:2005 it was far more in line with today's information security requirements. In the course of 2008, it was given the number ISO/IEC 27002:2005, in order to clearly tie it into the ISO/IEC 27000 series of information security management standards.

3.3 BS7799-2

BS7799-2:1999 was revised in 2002 and re-issued as BS7799-2:2002. The significant changes that occurred at this time included:

- the alignment of the clause numbering in both parts of the Standard;
- the addition of the PDCA model (see Chapter 15) to the Standard;
- the addition of a requirement to continuously improve the ISMS;
- the alignment of the Standard, and its detailed clauses, with ISO 9001:2000 and ISO 14001:1996, to facilitate the development of integrated management systems.

3.4 International adoption

BS7799-2:2002 was then adopted by the national standards bodies in a number of countries including Brazil, the Czech Republic, Finland, Iceland, Ireland, the Netherlands, Norway and Sweden and issued by them as their own national standards. For instance, the Australian and New Zealand standards bodies (Standards Australia and Standards New Zealand) jointly issued in 2003 a local version of BS7799-2:2002 under the number AS/NZS 7799.2.2003. Similarly, it was accepted by the South African Bureau of Standards as SABS 7799 / 2, in April 2002, while Spain developed its own version, UNE 71502:2004.

3) The IEC is 'the leading global organization that prepares and publishes international standards for all electrical, electronic and related technologies.' Its website is at www.iec.ch. The ISO and the IEC work together, within the World Trade Organization (WTO) framework, to provide technical support for the growth of global markets and to ensure that technical regulations, voluntary standards and conformity assessment procedures do not create unnecessary obstacles to trade. The joint ISO/IEC information centre has a website at www.standardsinfo.net/isoiec/index.html.

3.5 Translations and sector schemes

The Standard has also been translated into a number of languages, including Chinese, Czech, Danish, Dutch, Finnish, French, German, Icelandic, Japanese, Korean, Norwegian, Portuguese and Swedish. At the same time, a number of sector schemes have been developed. These are versions of BS7799-2:2002 that have been adapted and amended for specific sectors, such as the APACS Standard 55, the information security management standard now mandated by the UK payment services association for all its members.

3.6 ISO 27001:2005

BS7799-2 was still only a British Standard in June 2005, when ISO 17799:2005 was issued. The decision was taken, at that time, to put it on the 'fast track' to internationalization and FDIS (Final Draft International Standard) was issued in June 2005. BS7799-2:2005 (ISO/IEC 27001:2005) was finally published in October 2005.

It 'can be used to assess conformance by interested internal and external parties.' It is the specific document against which an ISMS can be assessed.

ISO/IEC 27001:2005 and ISO/IEC 27002:2005 still have the symbiotic relationship of a two-part standard.

