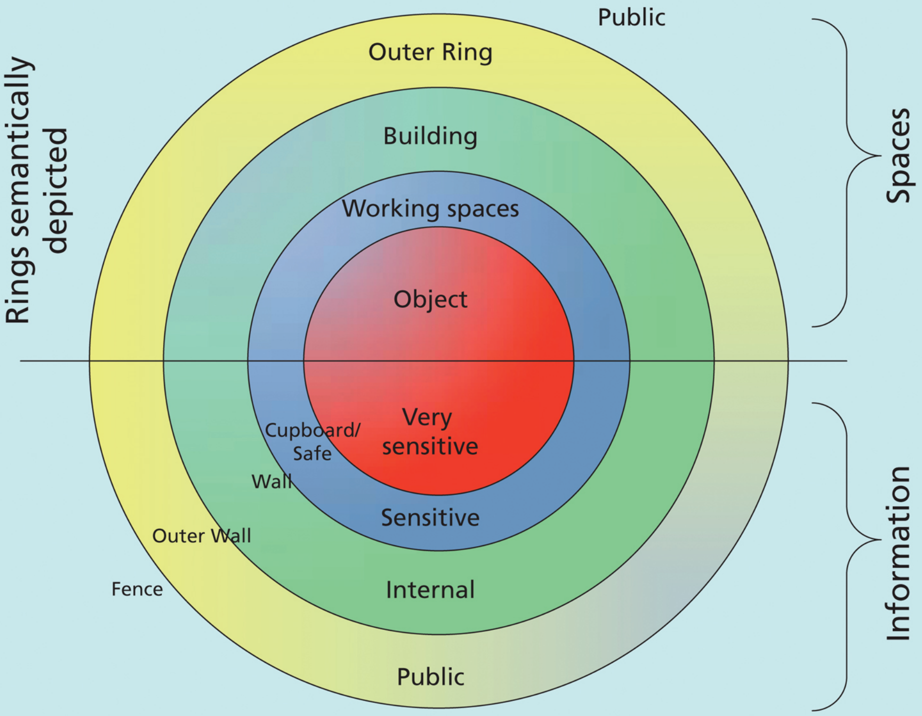
BEST PRACTICE

Foundations of Information Security

Based on ISO27001 and ISO27002

3RD, REVISED EDITION



Jule Hintzbergen
Kees Hintzbergen
André Smulders
Hans Baars

Van Haren PUBLISHING

Foundations of Information Security
3rd edition

Other publications by Van Haren Publishing

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

- IT and 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 materials etc. in the **Van Haren Publishing Knowledge Base**: www.vanharen.net for more details.

Van Haren Publishing is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi/NGN, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CATS CM®
CMMI®
COBIT®
e-CF
ISO 20000
ISO 27001/27002
ISPL
IT Service CMM
ITIL®
MOF
MSF
SABSA

Architecture (Enterprise and IT)

ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Business Management

BABOK® Guide
BiSL®
BRMBOK™
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
Novius B&IP
OPBOK
SAP
SixSigma
SOX
SqEME®

Project, Program and Risk Management

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP™
P3O®
PMBOK® Guide
PRINCE2®

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

Foundations of Information Security

Based on ISO 27001 and ISO 27002

3rd edition

Jule Hintzbergen
Kees Hintzbergen
André Smulders
Hans Baars

Van Haren
PUBLISHING

Colophon

Title:	Foundations of Information Security Based on ISO 27001 and ISO 27002 3rd edition
Series:	Best Practice
Authors:	Jule Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars
Reviewers 2nd edition:	- Norman Crocker (Cronos Consulting) - Steven Doan (Schlumberger, USA) - James McGovern (The Hartford) - Prof. Pauline C. Reich (Waseda University School of Law) - Bernard Roussely (Cyberens Technologies & Services) - Tarot Wake (Invictus Security)
Editor:	Steve Newton
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN Hard copy:	978 94 018 0012 9
ISBN eBook:	978 94 018 0541 4
Print:	Second edition, first impression, May 2010 Third edition, first impression, April 2015
Design and Layout:	CO2 Premedia, Amersfoort-NL
Copyright:	© Van Haren Publishing, 2010, 2015

For any further inquiries about Van Haren Publishing, please send an email 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.

Preface

The word ‘security’ has by its nature a negative feel to it. Security is, after all, only applied when there is reason to: when there is a risk that things will not go as they should. In this book various topics about IT security are explained, as simply as possible because IT security is everyone’s
responsibility, although many users of IT systems don’t realize this.

Security is not new, and indeed the roots for IT security are more than 2000 years old, for example the Egyptians used non-standard hieroglyphs carved into monuments and the Romans invented the so called ceasar cypher to encrypt messages. In addition, physical security is very old. Think about old fortresses and defenses like the Great Wall of China. In recent years physical security is more and more dependent upon IT and physical security is also necessary to protect information, so there IT comes together again.

The first edition of this book was published in 2011. The content was developed in close co-operation with EXIN. It was primarily intended as a study book for anyone in training for the EXIN exam *Information Security Foundation (based on ISO/IEC 27002).* But it is also suitable for anyone who would like to know more about IT security, since you can use it as awareness document for IT security. This book is intended to be read by everyone who wants to know more about IT security but also for people who want to have a basic understanding about IT security as a foundation to learn more.

The organization for Information Security Professionals in The Netherlands (PvIB) endorses this book as a very good start in the world of information security. It is a must read.

Fred van Noord, chairman PvIB (Platform voor Informatiebeveiliging) www.pvib.nl

Preface by the Authors

This is the third edition of this book that can be used to obtain an ISFS certification and it differs from the second edition in the way that it is based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

The ISO 27001:2013 standard has changed to meet the latest insights. The complete chapter structure has been changed to fit into the new standardized approach to ISO management standards. In addition, the standard not only focusses on the organization which uses the standard, but also on external stakeholders.

The 2013 version of ISO/IEC 27001 remains unchanged for the next five years. The overall approach of the management standards has been changed and the list of controls is modified. There are some additional changes:

- All management standards have the same chapter structure;
- There is a process for determining the correct scope of the ISMS through understanding the context of the organization;
- All definitions are now included in ISO 27000:2014;
- There are definitions of support metrics, such as the resources devoted to the ISMS;
- Greater visibility of leadership responsibilities;
- Annex A has changed to reflect the latest developments in ISO/IEC 27002:2013.

That brings us to ISO/IEC 27002:2013. The controls have major updates. Some are grouped, some are removed, some are changed and there are some new controls as well. The ISO/IEC JTC 1/SC 27 group that maintains the standards has created a document that maps the 2005 and 2013 revisions of the ISO/IEC 27001 and ISO/IEC 27002 and this document can be freely downloaded at: http://www.jtc1sc27.din.de/sixcms_upload/media/3031/ISO-IECJTC1-SC27_N13143_SD3_FINAL_TEXT_REV_2_Oct2013.pdf

This document will be helpful for those organizations who are looking for the changes and can help during the planning of activities aimed at modifying their information security management systems.

The authors team

Acknowledgements for second edition

This book has been written from the viewpoint that a basic understanding about IT security is important for everyone. We have tried to put a lot of information in this book without going into too much detail. Besides that, we are all Dutch guys and we were not able to write this book without the help of the reviewers who helped us to improve it.

We would like to thank the reviewers who provided us with valuable comments on the texts we had written. In alphabetical order they are:

- Norman Crocker, Cronos Consulting, Silves, Portugal
- Steven Doan, Schlumberger, Houston, Texas, USA
- James McGovern, The Hartford, Hartford, Connecticut, United States
- Prof. Pauline C. Reich, Waseda University School of Law, Tokyo, Japan
- Bernard Roussely, Director, Cyberens Technologies & Services, Bordeaux, France
- Tarot Wake, Invictus Security, Flintshire, United Kingdom

Contents

1 Introduction

This book is intended for everyone in an organization who wishes to have a basic understanding of information security. Knowledge about information security is important to all employees. It makes no difference if you work in a profit- or non-profit organization because the risks that organizations face are similar for all.

Employees need to know why they have to adhere to security rules on a day-to-day basis. Line managers need to have this understanding as they are responsible for the security of information in their department. This basic knowledge is also important for all business people, including those self-employed without employees, as they are responsible for protecting their own information. A certain degree of knowledge is also necessary at home. And of course, this knowledge forms a good basis for those who may be considering a career as an information security specialist, whether as an IT professional or a process manager.

Everyone is involved in information security, often via security countermeasures. These countermeasures are sometimes enforced by regulatory rules and sometimes they are implemented by means of internal rules. Consider, for example, the use of a password on a computer. We often view such measures as a nuisance as these can take up our time and we do not always understand what the measures are protecting us against.
Information security is the trick to find the right balance between a number of aspects:

- The quality requirements an organization may have for its information;
- The risks associated with these quality requirements;
- The countermeasures that are necessary to mitigate these risks;
- Ensuring business continuity in the event of a disaster;
- When and whether to report incidents outside the organization.

1.1 WHAT IS QUALITY?

First you have to decide what you think quality is. At its simplest level, quality answers two questions: 'What is wanted?' and 'How do we do it?' Accordingly, quality's stomping ground has always been the area of processes. From ISO 9000, to the heady heights of Total Quality Management (TQM), quality professionals specify, measure, improve and re-engineer processes to ensure that people get what they want. So where are we now?

There are as many definitions of quality as there are quality consultants, but commonly accepted variations include:

- 'Conformance to requirements' - P.B. (Phil) Crosby (1926-2001);
- 'Fitness for use' - Joseph Juran (1904 - 2008);
- 'The totality of characteristics of an entity that bear on its ability to satisfy stated and implied need' - ISO 9001-2008;
- Quality models for business, including the Deming Prize, the EFQM excellence model and the Baldrige award.

The primary objective of this book is to provide awareness for students who want to apply for a basic security examination. This book is based on the international standard ISO 27002:2013. This book is also a source of information for the lecturer who wants to question information security students about their knowledge. Many of the chapters include a case study. In order to help with the understanding and coherence of each subject, these case studies include questions relating to the areas covered in the relevant chapters. Examples of recent events that illustrate the vulnerability of information are also included.

The case study starts at a very basic level and grows during the chapters of the book. The starting point is a small bookstore with few employees and few risks. During the chapters this business grows and grows and, at the end, it is a large firm with 120 bookstores and a large web shop. The business risks faced by this bookshop run like a thread through this book.

This book is intended to explain the differences between risks and vulnerabilities and to identify how countermeasures can help to mitigate most risks. Due to its general character, this book is also suitable for awareness training or as a reference book in an awareness campaign. This book is primarily aimed at profit and non-profit organizations, but the subjects covered are also applicable to the daily home environment as well to companies that do not have dedicated information security personnel. In those situations the various information security activities would be carried out by a single person. After reading the book you will have a general understanding of the subjects that encompass information security. You will also know why these subjects are important and will gain an appreciation of the most common concepts of information security.