BEST PRACTICE

FOUNDATIONS OF INFORMATION SECURITY

BASED ON ISO27001 AND ISO27002

4th revised edition

Jule Hintzbergen, Kees Hintzbergen, Hans Baars

Van Haren PUBLISHING

Foundations of Information Security
4th 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 is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, CATS CM, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CMMI®
COBIT®
e-CF
ISM
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Project Management

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

Business Management

BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
CATS CM®
DID®
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

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

Foundations of Information Security

Based on ISO 27001 and ISO 27002

4th fully revised edition

Jule Hintzbergen
Kees Hintzbergen
Hans Baars

Van Haren PUBLISHING

Colophon

Title:	Foundations of Information Security based on ISO 27001 and ISO 27002 - 4th edition
Series:	Best Practice
Authors:	Jule Hintzbergen, Kees Hintzbergen, Hans Baars
Publisher:	Van Haren Publishing, 's-Hertogenbosch, www.vanharen.net
ISBN Hard copy:	978 94 018 0958 0
ISBN eBook:	978 94 018 0959 7
ISBN ePub:	978 94 018 0960 3
Print:	Second edition, first impression, May 2010 Third edition, first impression, April 2015 Third edition, second impression, September 2017 Fourth edition, first impression, February 2023
Design and Layout:	Coco Bookmedia, Amersfoort - NL
Copyright:	© Van Haren Publishing, 2010, 2015, 2017, 2023

For any further inquiries about Van Haren Publishing, please send an email to: info@vanharen.net

Preface by the authors

This is the fourth edition of this book that is designed to help you learn more about information security and can help you achieve the ISFS certification of EXIN. The difference with the previous (3rd) edition is that this edition is based on a totally revised version of the ISO 27002 standard, released in 2022.

A revision of the ISO 27002 standard is usually limited to some new topics, the removal of certain obsolete terms or techniques and adjustments to the changes in times. For example, the floppy disk, mentioned in the first edition, disappeared over time and in the 2013 edition the topic of cryptography was added as a new chapter.

However, the new 2022 version of the ISO 27002 standard was a major revision of the previous version. It merged 24 topics and added 13 new measures (controls). The biggest changes, however, were the reduction of 14 chapters to 4 chapters within which the measures were regrouped. These four chapters are now called Themes. This means that the standard has been completely redescribed and reorganized. The structure of the measure description was also addressed. There were two reasons for this:

1. The 2013 version of the ISO 27002 standard had become more and more of a checklist in recent years. The purpose of each measure, specified in this version, was no longer carefully considered, but rather limited to the question whether the measure had been implemented and then it was ticked off as 'done'. However, there is a difference between implementing the cheapest virus scanner and not updating it daily or finding out which virus scanner offers the best protection in your specific situation and making sure it is kept up to date in a daily update cycle. We can think of a similar example for almost every issue in this standard.
2. People started looking at things differently after the introduction of the ISO 27002 standard in the 1990s. People now think more in terms of themes, attributes and KPIs. The 2022 version of the ISO 27002 standard responds to this and allows security professionals to think more and better about the way they want to shape security for their company. However, many will have to get used to the new format.

This fourth edition adopts the new ISO 27002:2022 standard and will serve as a guide over the next few years for those who are going to delve into the subject, and certainly for those who are going to (re)certify for ISO 27001.

ISO 27002 has been renamed. The old title was "Information Technology - Security Techniques - Code of Practice for Information Security Controls". The title of the 2022 edition is: "Information security, cybersecurity and privacy protection - Information security controls". The phrase "Code of Practice" has been removed from the title of this document to better reflect the purpose of the document. It is a reference set of information security controls.

The purpose of the ISO 27002:2022 standard has not changed from the old versions of 2013-2020. The intent of the ISO/IEC 27002 standard is still the same: helping organizations ensure that necessary measures are not overlooked.

One of the goals of the ISO/IEC 27002 standard is for organizations to fine-tune their own information security management. As always, the concepts of Availability, Integrity and Confidentiality are an integral part of the ISO 27002. However, this has now been joined by the five attributes from the ISO 27103, describing a cybersecurity framework, introduced in 2018: Identify, Protect, Detect, Respond and Recover. Such a value is preceded by a "#" making it easy to find an attribute or to filter on such an attribute. This, among other things, has made the new version of the ISO/IEC 27103 standard, introduced in 2018, an integral part of ISO/IEC 27002.

The authors team

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 businesspeople, 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.

In information security the goal is 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;
- establishing when and whether to report incidents outside the organization.

1.1 MAJOR CHANGES IN THE ISO/IEC 27002:2022

1.1.1 ISO/IEC 27002: 2013 Control layout

The 2013 version of ISO/IEC 27002 and the updates during the years up to 2020 had four introductory chapters and 13 chapters including security guidelines: chapters 5 through 18. Each chapter contains sections containing a "purpose" and one or more subsections including a control and an implementation guideline.

The Annex Table B2 of ISO/IEC 27002:2022 is a comparison table and gives a complete overview of the changes that took place between the 2013 version and the 2022 version.

1.1.2 ISO/IEC 27002: 2022 Control layout

The new version of the ISO 27002 has a different format. Where the old 2013 version consisted of 14 categories, the new 2022 version only has 4 categories left. In addition, these are more logically grouped, based on the most logical department or area of responsibility of an organization where these controls should belong.

In addition, five security aspects were added per control: Control type, Information security properties, Cybersecurity concepts, Operational capabilities and Security domains.

Organizations who have setup their ISMS based on the old ISO numbering will have serious work in changing their documentation where the old ISO numbering is used as reference.

Table 1.1 Security aspects

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ Ecosystem #resiliance

The goal of this division is for the company's security manager to start thinking about CIA (Confidentiality, Integrity, Availability) classifications: will these remain leading? Or are we going to group the security measures around the five cybersecurity aspects? This division is intended to prevent the ISO 27002 from becoming a checklist. The security manager is now forced to make choices and have them substantiated in the event of certification. Section 3.5 explains these concepts in more detail.

As can be seen in Table 1.1, each of the aspects are preceded by a #. This is meant to allow for a quick search on such an aspect. Would you search on 'integrity', then 214 results come up. However, if you search on #Integrity, 177 results remain, which are directly linked to a security measure.

1.2 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 the ISO 9000 standard, 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 9001:2015;
- 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 27002:2022. This book is also a source of information for the lecturer or trainer 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 Springbooks 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.

2 Case study: Springbooks – An international bookstore

2.1 INTRODUCTION

To understand the theory in this book, it will be helpful to translate it to a practical situation. In most situations the reader gets a better understanding of the theory when it is illustrated by a practical case study.

In this case study, used throughout all chapters of this book, questions are included that relate to lessons learned in each chapter.

Figure 2.1 Springbooks' London headquarters

This chapter gives an explanatory introduction to the case study. The establishment of the bookstore, the history and the years of growing into an international company are all described.

Springbooks was founded in 1901. During its expansion into an international organization operating within Europe the company had to change and to adjust to its environment. A major part of this is the huge change over the last 50 years in supplying information. As one might imagine there is a big difference in process control between the time Springbooks was founded in 1901, with the emergence of Information and Communication Techniques (ICT) during the 1960s and 1970s, through to

the ever-increasing dependence on ICT nowadays. ICT has become one of the most important tools for Springbooks.

Now in the 2020s Springbooks IT is in the Cloud and the web shops turnover is greater than that of the physical shops. The board of directors is aiming for ISO 27001 certification by the end of this year.

2.2 SPRINGBOOKS

Springbooks Ltd. (SB) is a European operating bookstore. SB is an organization with 120 bookshops, most of which are run on a franchise basis. In total, 50 of the shops are owned by SB itself.

Figure 2.2 Organizational chart Springbooks 1901-1931

SB was founded in 1901 when Henry Spring opened a small shop in Bedrock-on-Thames, UK.

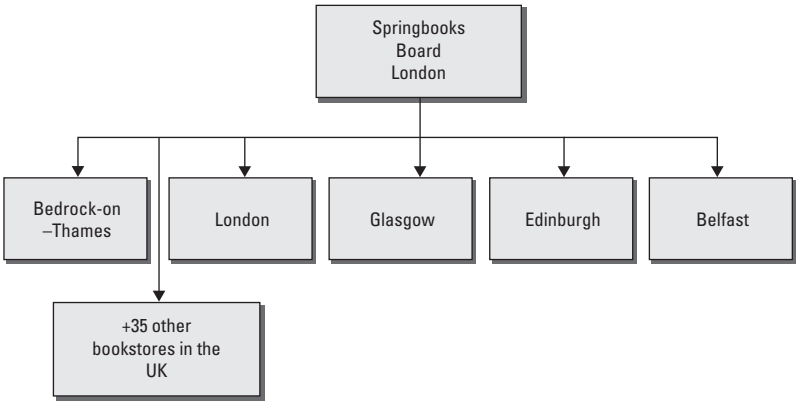

Figure 2.3 Organization of Springbooks 1938

Over time 36 shops were established in all major cities in the UK. Immediately after the end of World War 2 SB established bookshops in Amsterdam, Copenhagen, Stockholm, Bonn, Berlin and Paris.

Nowadays SB has shops in all major cities in the EU. The Board of Directors is based at offices in London. Because of the Brexit an independent European headquarter is established in Amsterdam. Every country has a central office. All bookstores are accountable to their national office.

The national office is accountable to the European Headquarters in Amsterdam.
The European headquarters are ultimately accountable to the Board of Directors in London.

In 2020 plans were made to expand the international business into the USA and Canada. New branches however have been canceled due to the Corona crisis. The board expects to be able to implement the plans in the near future.

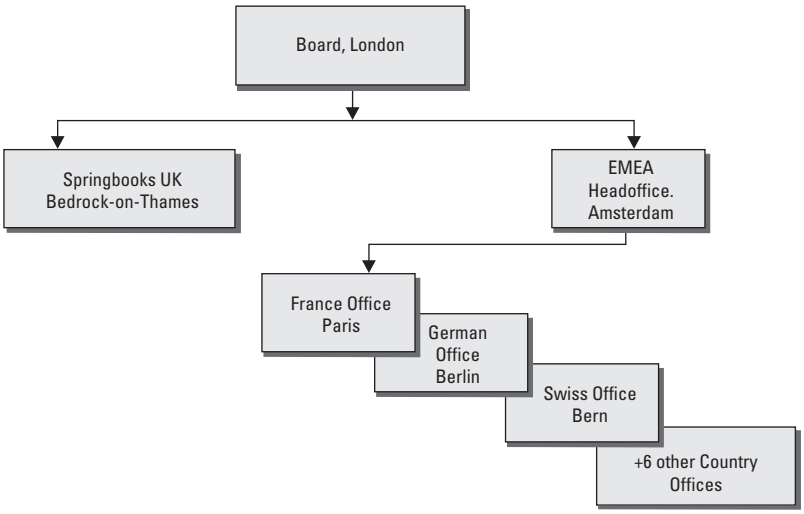

Figure 2.4 Organization of Springbooks 1946-2022

The board of directors has adopted an old-fashioned approach to business for a long time. The Internet was not their way of doing business.

In 2013 an independent consultancy group has advised that SB should launch stores in Australia and New Zealand to expand in combination with the very successful 'local' Internet stores which were opened in Australia and New Zealand in 2014. Because of this success SB has now one of the world's most successful internet stores where the 2020 turnover consists of 60% eBooks and 40% physical books in addition to magazines.

2.3 ORGANIZATION

London UK:
In the London Headquarters resides the Board of Directors and the overall Chief Information Officer (CIO), Chief Financial Officer (CFO), Chief Procurement Officer (CPO) and Chief Executive Officer (CEO).

Each country has a central office which is responsible for the business in that specific country. The Country Director is responsible to the Unit Director for their particular region.