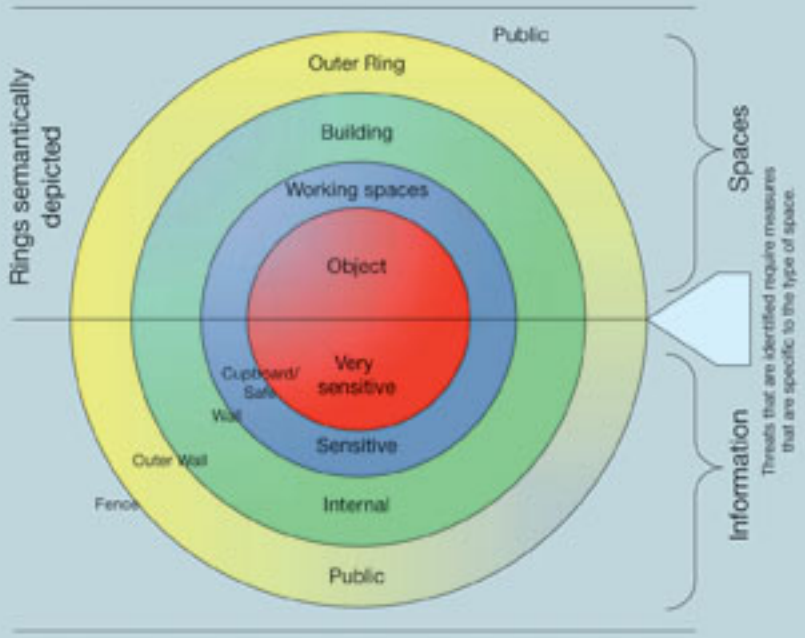
BEST PRACTICE

Foundations of Information Security

Based on ISO27001 and ISO27002



Jule Hintzbergen
Kees Hintzbergen
André Smulders

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

VHP is also publisher on behalf of leading companies and institutions:
The Open Group, IPMA-NL, PMI-NL, CA, Getronics, Quint, ITSqc, LLC, 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 27002
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®
eSCM

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

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

Foundations of IT Security

Based on ISO27001/27002

Jule Hintzbergen

Kees Hintzbergen

André Smulders

Hans Baars

Van Haren PUBLISHING

Colophon

Title:	Foundations of IT Security
Subtitle:	Based on ISO27001/27002
Series:	Best Practice
Authors:	Jule Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars
Editor:	Steve Newton
Reviewers:	- 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)
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 568 1
Print:	Second edition, first impression, May 2010
Design and Layout:	CO2 Premedia, Amersfoort-NL
Copyright:	© Van Haren Publishing, 2010, excluded appendix B
Printer:	Wilco, Amersfoort-NL

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

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 mentioned, 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 can be found centuries ago when, 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.

This book started originally two years ago in Dutch and then there couldn't be found a way to get it to you out there. The book was adapted by EXIN as study book and 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. The first translation to English never made it, and needed a lot of rework. This book is intended to be read by everyone who wants to know more about IT security but also for people that want to have a basic understanding about IT security as a foundation to learn more.

What do you find in this book?
At first there are basic understanding and address common topics such as the fundamental principles of security and information security, and risk management. From there the book goes on to look at the architecture, processes and information that are needed for a basic understanding of what IT security is about. We then go deeper in threats and risks together with risk management.

Business assets are then discussed, what are they and how should they be used and maintained? Later chapters are about the measures that can be taken to protect IT assets. Firstly we mention physical measures, that's were it all starts, the door to go into a building. Secondly we mention the technical measures, including encryption. Thirdly we mention the organizational measures. Organizational security measures are often inextricably linked with technical measures. Where relevant, we will refer to the technical measures that are necessary in order to be able to carry out or enforce these organizational measures.

Finally we write about managing the communication and operating procedures that are necessary for the effective management and control of the IT within an organization.

We also include some information about law and regulations. This is an international book and we cannot put everything in there. To find more about local laws we suggest you look on the Internet.

This book is recommended as a study book for the Information Security Foundation based on ISO/IEC 27002 exams of EXIN.

EXIN is an independent, international examination institute for IT professionals. EXIN's mission is to improve the quality of the IT sector as well as that of IT professionals. In order to achieve these goals, EXIN develops exam requirements and IT exams. EXIN provides four examinations in Information Security. These examinations are based on ISO/IEC 27002. You can take exams at Foundation, Advanced and Expert level. At the Expert level you are tested not only on your knowledge of ISO/IEC 27002 but also that of ISO/IEC 27001.

The organisation for Information Security Professionals in The Netherlands (PvIB) endorse 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

Acknowledgements

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

Content

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 equal for all organizations.

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 experience measures as a nuisance as these can take up our time and we do not always know what measures they are protecting us against.

The trick to information security is finding the right balance between a number of aspects:
- The quality[1] 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.

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' – Crosby;
- 'Fitness for use' – Juran;
- 'The totality of characteristics of an entity that bear on its ability to satisfy stated and implied need' - ISO 8402:1994;

1 http://syque.com/articles/what_is_quality/what_is_quality_1.htm

- Quality models for business, including the Deming Prize, the EFQM excellence model and the Baldrige award.

The primary objective of this book is to achieve awareness by students who want to apply for a basic security examination. This book is based on the international ISO 27002 Code of Practice for this information security standard.

This book is also a source of information for the lecturer who wants to question information security students about their knowledge. Each chapter ends with 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 are 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 has 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, during the emergence of Information and Communication Techniques (ICT) during the 1960's and 1970's, through to the ever increasing dependence on ICT nowadays. ICT has become one of the most important tools for Springbooks.

2.2 Springbooks

Springbooks Ltd. 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.

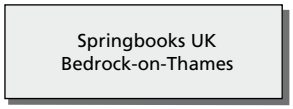


Figure 2.2 Organizational Chart Springbooks in 1901

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

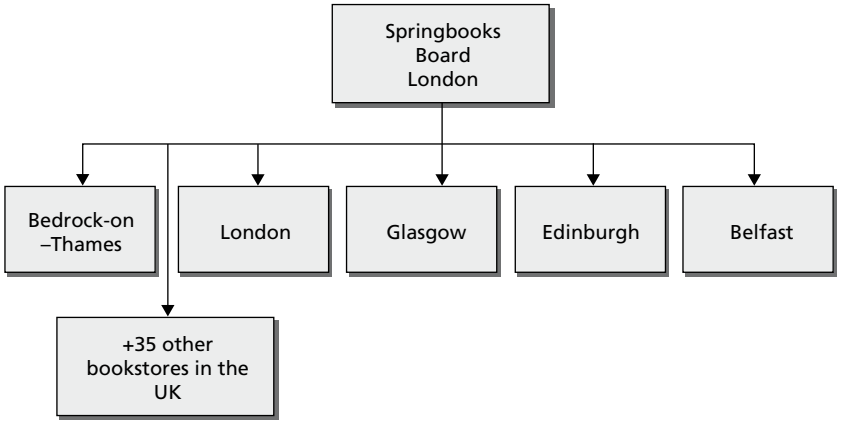


Figure 2.3 Organization of Springbooks 1938

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

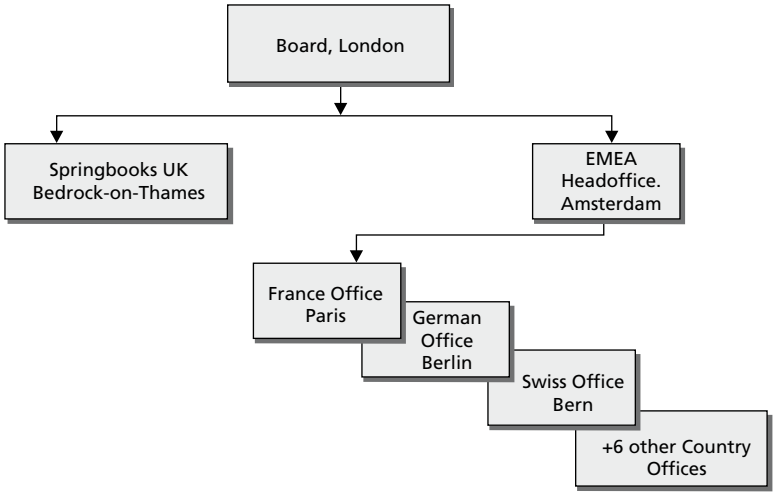


Figure 2.4 Organization of Springbooks 1960

Nowadays SB has shops in all major cities in the EU. The Board of Directors is based at offices in London. European headquarters are in Amsterdam and 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 2000 plans are made to expand the international business into the USA, Canada, Australia and New Zealand by the end of the first decade of 2000. However, because of the banking crisis which arises at the end of 2008, these plans are not carried out, at this moment.

The banking crisis has had a serious affect upon the worth of SB shares. The fact is that one of the first things people economize on are books, newspapers and magazines. All these are core businesses of SB. This resulted in a temporary halt on the plans to expand the overseas market. Investment plans in new stores are frozen and a search for new markets has resulted in new plans.

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.

However, an independent consultancy group has advised that SB should launch an online store and not limit sales to simply books, and magazines, but instead look to expand into travel in combination with travel books and, in the longer term, also offer consumer electronics and other consumer goods.

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.

Bedrock-on-Thames UK:
UK Director (UK is not EU) responsible for the UK bookstores. There is also an UK-CIO, CEO, CFO and a Local Information Security Officer (LISO).

Amsterdam, the Netherlands:
1 EU director (EU without UK)

EU CIO, CEO, CFO, CPO, LISO and the Corporate Information Security Officer (CISO).
Springbooks has a partly centralized information security organization. The main way of performing (or handling) information security is directed out of the London headquarters. ISO 27001 and ISO 27002 are the standards to be used in all countries.

In London, there is a Corporate Information Security Manager who has overall responsibility for organizing information security in the corporation. He ensures that information security is part of the daily job of all Springbooks employees.

It is up to the local offices to ensure compliance with local law and regulations. This decentralized part of information security can have an impact on the way information security has to be organized locally.

The national Local Information Security Officer (LISO) is responsible for adherence to both the central rules, and the national rules. He is also responsible for the physical security of the bookstores and Health Safety and Environment of the bookstore employees. In the UK next to the CISM, the LISO is responsible for the information security at the UK bookstores.

Every bookstore has an information security focal point. This is an employee who is accountable for information security in the store and the contact point to the 'national' LISO.

IT is centrally organized. There is a wide area network (WAN) that all stores are connected to. The Springbooks wide area network (WAN) is a computer network that covers a broad area. This is in contrast with local area networks (LANs) in the bookstores that are limited to a single building.

The cash desks are connected to this WAN. Every book that is sold is scanned at the cash desk and registered in a central database. This makes it possible to have an accurate overview of books in stock every (part of the) day. By updating stocks based on sales, Springbooks can ensure that the popular books are always in stock. The speed of restocking depends on the popularity of the book, of course.

Every employee has their own ID that is used to login to the cash desk system. Every book sold, is connected to the employee who produced the invoice. In the same database there is a lot of customer information stored, such as names, addresses and credit card information.

All customer-related information stored in the Springbooks' IT environment makes information security and compliance to (national) privacy laws very important. Unexpected and unauthorized disclosure of the customer database can have huge consequences for the trustworthiness of Springbooks.

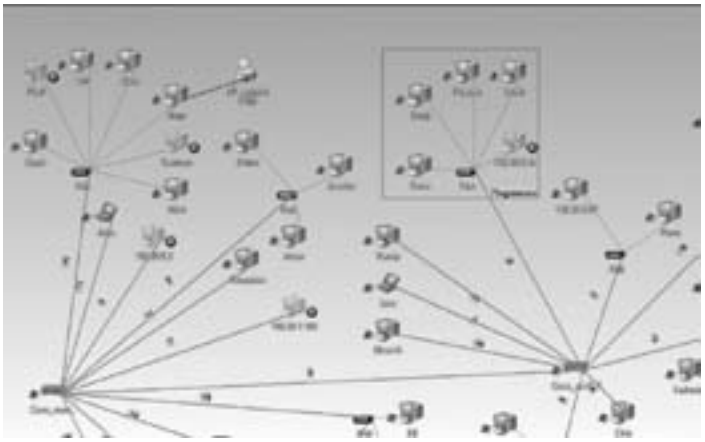


Figure 2.5 Data connections between bookstores are speeding up

3. Definitions

This chapter contains definitions of key concepts in the book. In Appendix A you will find an extensive glossary.

Asset
Anything that has value to the organization.
[ISO/IEC 13335-1:2004]

Availability
Availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when needed. In addition this concept guarantees that the security services that the security practitioner requires are in working order. [2]

Confidentiality
The concept of confidentiality attempts to prevent the intentional or unintentional disclosure of a message's content. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication in network rights.

Control
A means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature.
NOTE Control is also used as a synonym for safeguard or countermeasure.

Exposure
An exposure is an instance of being exposed to losses from a threat agent.

Information
Information is data that has meaning in some context for its receiver. When information is entered into and stored on a computer, it is generally referred to as data. After processing (such as formatting and printing), output data can again be perceived as information.

Information analysis
Information analysis provides a clear picture of how an organization handles information—how the information 'flows' through the organization.

Information management
Information management describes the means by which an organization efficiently plans, collects, organizes, uses, controls, disseminates and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent.

Information processing facilities
Any information processing system, service or infrastructure, or the physical locations housing them.

Information security
Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

2 The CICCP Prep Guide, Ronald L. Krutz / Russel Dean Vines More information can be found in chapter 4

Information security event
An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security-relevant.
[ISO/IEC TR 18044:2004]

Information security incident
An information security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
[ISO/IEC TR 18044:2004]

Information security management
Coordinated activities to direct and control an organization with regard to risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.
[ISO/IEC Guide 73:2002]

Information system
In a very broad sense, the term information system is frequently used to refer to the interaction between people, processes, data and technology. In this sense, the term is used to refer not only to the information and communication technology (ICT) an organization uses, but also to the way in which people interact with this technology in support of business processes.

Integrity
The concept of integrity ensures that unauthorized modification to software and hardware is prevented, unauthorized modification is not made to data by authorized and unauthorized personnel and/or processes and that data is internally and externally consistent.

Policy
The overall intention and direction as formally expressed by management.

Risk
A combination of the probability of an event and its consequence.

Risk analysis
The systematic use of information to identify sources and to estimate the risk.

Risk assessment
The overall process of risk analysis and risk evaluation.

Risk evaluation
The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk treatment
The process of selection and implementation of measures to modify risk.

Third party
The person or body that is recognized as being independent of the parties involved, as far as the issue in question is concerned.
[ISO/IEC Guide 2:1996]

Threat
A potential cause of an unwanted incident, which may result in harm to a system or organization.
[ISO/IEC 13335-1:2004]

Vulnerability
A weakness of an asset or group of assets that can be exploited by one or more threats.