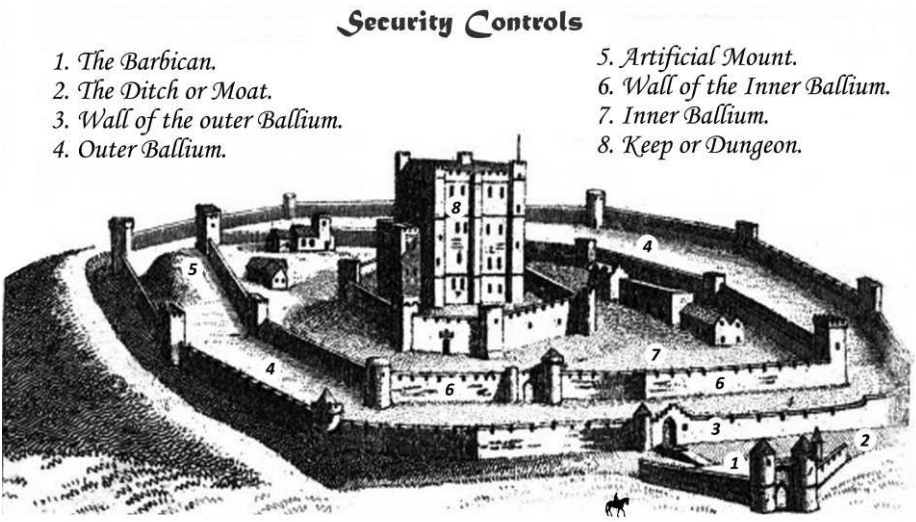
ISO 27001 handbook

Implementing and auditing an
Information Security Management System
in small and medium-sized businesses



Publisher: Deseo / Brave New Books
ISBN 9789402115116
BISAC COM053000
NUR 982
Version: 20200209
Keyword: Information security

Book cover: Rob Westendorp – WSTNDRP
Photo author: Heleen Rozeveld
Book pictures: Cees van der Wens
Editors: Book Helpline
Cover illustration: iStock.com/Physicx

Contents

Introduction

About this book

This handbook is intended to help small and medium-sized businesses establish, implement, maintain and continually improve an information security management system in accordance with the requirements of the international standard ISO/IEC 27001.

At the same time, this handbook is also intended to provide information to auditors who must investigate whether an information security management system meets all requirements and has been effectively implemented.

The reason that this handbook focuses on SMBs is that an information security management system must be set up there in a different way than in large organizations. An SMB must meet the same requirements, but the management system must be suitable for a company that is smaller and more agile.

Certification

This handbook assumes that you ultimately want your information security management system to be certified by an accredited certification body.

The moment you invite an accredited certification body to perform a certification audit, you must be ready to demonstrate that your management system meets all the requirements of the Standard. In this book, you will find detailed explanations, more than a hundred examples, and sixty-one common pitfalls. This book also contains information about the rules of the game and the course of a certification audit.

Certification should not be an objective in itself. A non-certified management system can also be an excellent tool for effectively organizing information security.

Reading guide for this book

The numbers and titles of chapters four to ten of this book, correspond to those used in the Standard, enabling you to use the book and the Standard side by side.

Chapters four to ten each deal with one or more clauses of the Standard. For example, chapter six consists of the clauses 6.1.1, 6.1.2, 6.1.3 and 6.2. Each clause contains one or more requirements. Requirements are conditions that you must meet in order to be allowed to claim conformity with the Standard.

When reading chapters four to ten of this book, you will see that the Standard is followed closely, but the actual text is not provided. The reason for this is that this book is not a substitute for the Standard. To get to know the requirements in detail, you will need to purchase a copy of the Standard.

In order not to introduce any additional noise, this book keeps the use of words deliberately as close as possible to the Standard. Where necessary, this book explains specific words and concepts. Paragraphs that begin with the symbol ➢ are intended as clarification or addition to the main text.

Chapters four to ten in this book each start with a schematic representation of the Standard. In each picture, the relevant clauses are marked. The pictures are from the author of this book; they are not from the Standard.

Within chapters four to ten, the following fixed topics are discussed for each clause:

- *Explanation, examples, and pitfalls*
  What requirements are there in this clause? What do they mean? What do you have to do? What should you not do?
- *Mandatory documentation*
  What documented information does this clause require?
- *Instructions for performing audits*
  What could an (internal) auditor investigate concerning the requirements of this clause?

The “instructions for performing audits” are intended to help you meet the requirements of clause 9.2. This clause requires you to perform internal

audits at scheduled intervals to determine whether your information security management system meets all requirements and is effectively implemented and maintained. The instructions at the end of each clause contain specific information for conducting internal audits.

This book follows the Standard closely, but where the Standard stops after Annex A, this book continues for a few chapters. These additional chapters are intended to give you practical tips and other useful information.

Sometimes you will come across a block with a number, for example: [3]. This number refers to one of the sources used by the author. The Sources chapter at the end of this book provides details for each source.

Disclaimer

The explanations and examples in this book stem from personal opinions and experiences of the author and can be challenged by others. The author cannot be held responsible for any negative consequences that may arise from applying the information in this book.

1. The ISO/IEC 27001 Standard

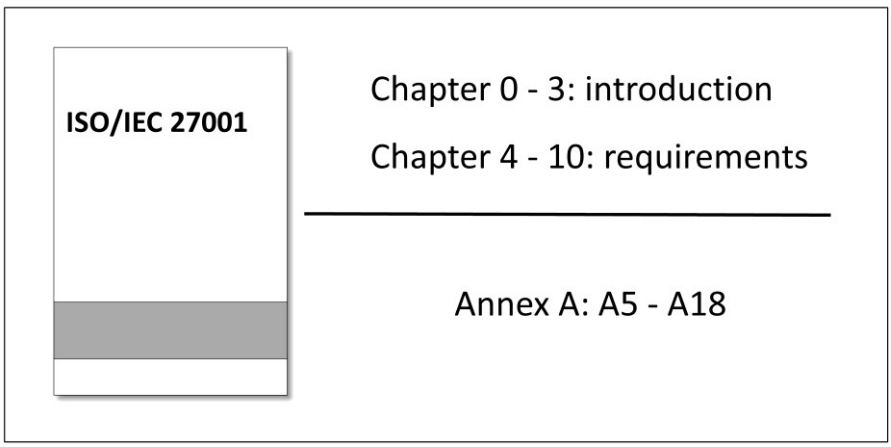
THE USE OF THE STANDARD

The ISO/IEC 27001 standard is a document of around thirty pages that you can buy on the internet. The standard is international and is, therefore, available in many languages. The English standard contains the source text from which all translations are derived.

The ISO/IEC 27001 standard is a publication of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC is a system that specializes in worldwide standardization.

The name ISO/IEC 27001 is often shortened to ISO 27001 (see also the title of this book). In this book, the ISO/IEC 27001 will be referred to almost throughout as "the Standard."

The Standard is not easy to understand, especially for beginners. It contains no checklists and hardly gives any explanation as to what you should do. The intention is for you to give meaning to the content of the Standard yourself; one that fits your specific activities, obligations, risks, and objectives. This book is intended to help you with this.



STRUCTURE OF THE STANDARD

In chapters zero to three of the Standard, you will find introductory information. It can be enlightening to read this information.

Chapters four to ten of the Standard describe the requirements that you must meet to be allowed to claim conformity with it.

The Standard also has an Annex A. The control objectives and controls listed in this Annex A are directly derived from and aligned with those listed in document ISO/IEC 27002 [3].

WHAT IS MANDATORY? WHAT IS NOT?

Chapter 1 of the Standard tells you that excluding any of the requirements specified in clauses 4 to 10 is not acceptable. So whatever type of organization you are, all these requirements are mandatory.

What about Annex A of the Standard? Do you have to comply with everything in it? It depends. This book explains in detail how to deal with Annex A (see clause 6.1.3).

WHAT DOES THE STANDARD MEAN BY THE WORD "ORGANIZATION?"

Chapter one of the Standard also tells you that the requirements in the Standard are intended to be applicable to all organizations, regardless of type, size or nature. What is meant by the word *organization*?

The term *organization* includes but is not limited to sole trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private [1].

Note that an organization does not have to be a legal entity and that an information security management system is also applicable to a sole trader.

WHY ARE THE REQUIREMENTS IN THE STANDARD SO VAGUE?

Section 0.1 of the Standard tells you that "the order in which the requirements are presented does not reflect their importance or imply the order in which they are to be implemented." That sounds like a cookbook telling you that the order in which the ingredients are presented in the recipes does not reflect their importance or imply the order in which they are to be used.

Besides the fact that the order of requirements can be confusing, the requirements themselves are generally perceived as vague. This vagueness often raises many questions. Why doesn't the Standard tell me more precisely what to do? Why do I have to find out for myself?

The main cause of the "vagueness" is that the Standard is intended for all types of organizations and that the requirements cannot be too specific. For example, the Standard requires that there must be an information security policy, but not what it must contain. That depends, after all, on what policy is needed within your organization. Nor can the Standard prescribe specific technical and organizational measures because what is necessary depends on your specific information security risks.

This is why you must implement an information security management system that meets the Standard, that fits your activities, obligations, risks, and objectives, and that can be integrated with your business processes and management structure. That is quite a bit, and in practice, this is not always easy. This book is intended to help you with it.

Another reason why the Standard sometimes seems somewhat puzzling is that ISO/IEC would rather not explain things that have already been described in other ISO/IEC documents. This book sometimes refers to these documents (see also the chapter *Sources* in this book).

HIGH-LEVEL STRUCTURE (HLS)

Section 0.2 of the Standard discusses the *compatibility* of the ISO/IEC 27001 standard with other ISO/IEC management system standards. What's the meaning of this?

The ISO/IEC 27001 standard is not the only ISO/IEC management system standard. Other management system standards are ISO/IEC 9001 (quality), ISO/IEC 14001 (environment) and ISO/IEC 22301 (business continuity).

The ISO/IEC 27001 standard uses the so-called *High-Level Structure* (HLS). That is, the Standard uses identical section titles, sub-clause titles, text, common terms and core definitions as the other ISO/IEC management system standards. This approach is useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

➢ *This book does not pay special attention to combining multiple management system standards.*

ISO/IEC 27000

Chapters two and three of the Standard inform you about the existence of the document ISO/IEC 27000 (see also Sources [1]). This document contains definitions that can be used to get more clarity about the meaning of specific terms used in the Standard. This book sometimes refers to this document.

BIBLIOGRAPHY

At the end of the Standard, a list of documents is included under the title *Bibliography*. These documents offer additional information on the ISO/IEC 27001 standard.

Just like this book, document ISO/IEC 27003 contains guidelines for implementing the Standard, but the information in that document is minimal. This book sometimes refers to that document (see also Sources [4] in this book).

2. Information Security

The concept of *information security* can be broken down into the following three dimensions [1]:

- The preservation of the *confidentiality of* information
- The preservation of the *integrity* of information
- The preservation of the *availability* of information

These three guiding principles behind information security are often abbreviated as CIA.

PRESERVING THE CONFIDENTIALITY OF INFORMATION

When it comes to information security, the term *confidentiality* is usually mentioned first. Confidentiality is the property that information is not made available or disclosed to unauthorized persons, entities or processes [1]. Confidential information may include personal data but also other types of information such as trade secrets or competition-sensitive data.

A loss of confidentiality of information can occur in many ways. Organizations can share their clients' confidential information with others without permission, and an e-mail with confidential information can be sent to the wrong person by mistake. People with malicious intent can steal or copy confidential information and take advantage of it. People can consciously or accidentally share confidential information in a conversation. A stolen, lost or carelessly discarded computer can contain a wealth of confidential information.

Pitfall 1 "Information security is about confidentiality"

It is often thought that information security is only about preserving the confidentiality of information. However, within the context of the Standard, information security is also about preserving the integrity and availability of information.

PRESERVING THE INTEGRITY OF INFORMATION

The *integrity* of information is about the accuracy and completeness of information [1]. The word integrity sometimes leads to confusion because it also exists outside the context of information security, namely in the form of personal property (honest, sincere). You could say that "honest" information is accurate and complete.

A loss of integrity of information can occur due to incorrect input, processing or presentation of data (manually or automated). People with malicious intent can deliberately compromise the accuracy and completeness of information to benefit or to cause harm. Someone can restore a wrong backup with the result that information is no longer correct or complete. Remember that even large banks occasionally face the problem of incorrect bank accounts.

PRESERVING THE AVAILABILITY OF INFORMATION

When it comes to information security, the *availability* aspect is often mentioned last. Not because the availability of information is considered unimportant, but because it is not always immediately linked to the protection of information. Preserving availability is about making information accessible and usable upon demand by an authorized entity [1] (the organization or person who wants and may have access to the information).

A loss of availability of information can be temporary or permanent. It can be caused by unintended causes such as incorrect actions, technical malfunctions or natural disasters. People with bad intentions can destroy information, make it inaccessible or make it unreadable. Information systems can become overloaded. Someone can set up a DDoS attack to intentionally disrupt information systems. Information carriers such as paper, tapes, hard writing, and USB sticks can lose their information due to aging. Sometimes, information is no longer available because a deceased person was the only person who knew specific passwords.

OTHER ASPECTS

Other properties can also be involved in information security, such as [1]:

- *Non-repudiation*: This refers to the ability to prove that a claimed event or action has occurred. For example, getting a signature on a receipt when delivering a postal package.
- *Authenticity:* This is the property that an entity is what it claims to be. For example, the use of a digital certificate that ensures that someone knows that messages come from a particular sender (source authenticity).
- *Reliability*: This refers to the property of consistent intended behavior and consistent results. For example, information that sometimes appears quickly and sometimes slow on a screen, or information of which the content is continually changing, when this is unintended.

INFORMATION SECURITY AND THE GDPR (EUROPE)

The concept of information security can relate to all types of information, including personal data.

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).

GDPR article 32 is about the "security of personal data." The article states:

> *"The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (…) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."*

As you will see when reading this book, "implementing technical and organizational measures to ensure a level of security appropriate to the risk" and "regularly testing, assessing and evaluating the effectiveness of technical and organizational measures" is entirely in line with the ISO/IEC 27001 approach.

➢ *The GDPR is about many more topics than Personal Data Security. The ISO/IEC 27001 standard does not cover all GDPR requirements.*

This book is not about the GDPR, but will occasionally refer to it.

3. Management System

SYSTEM

Organizing information security is becoming increasingly complex. The systematic management of information security has therefore become a necessity.

The Standard starts with chapter zero. In section 0.1, you can read that the Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an *information security management system*. This system is intended to preserve the confidentiality, integrity, and availability of your information (see also chapter two of this book).

To start slowly with setting up your *information security management system*, this chapter includes some general information.

ISMS

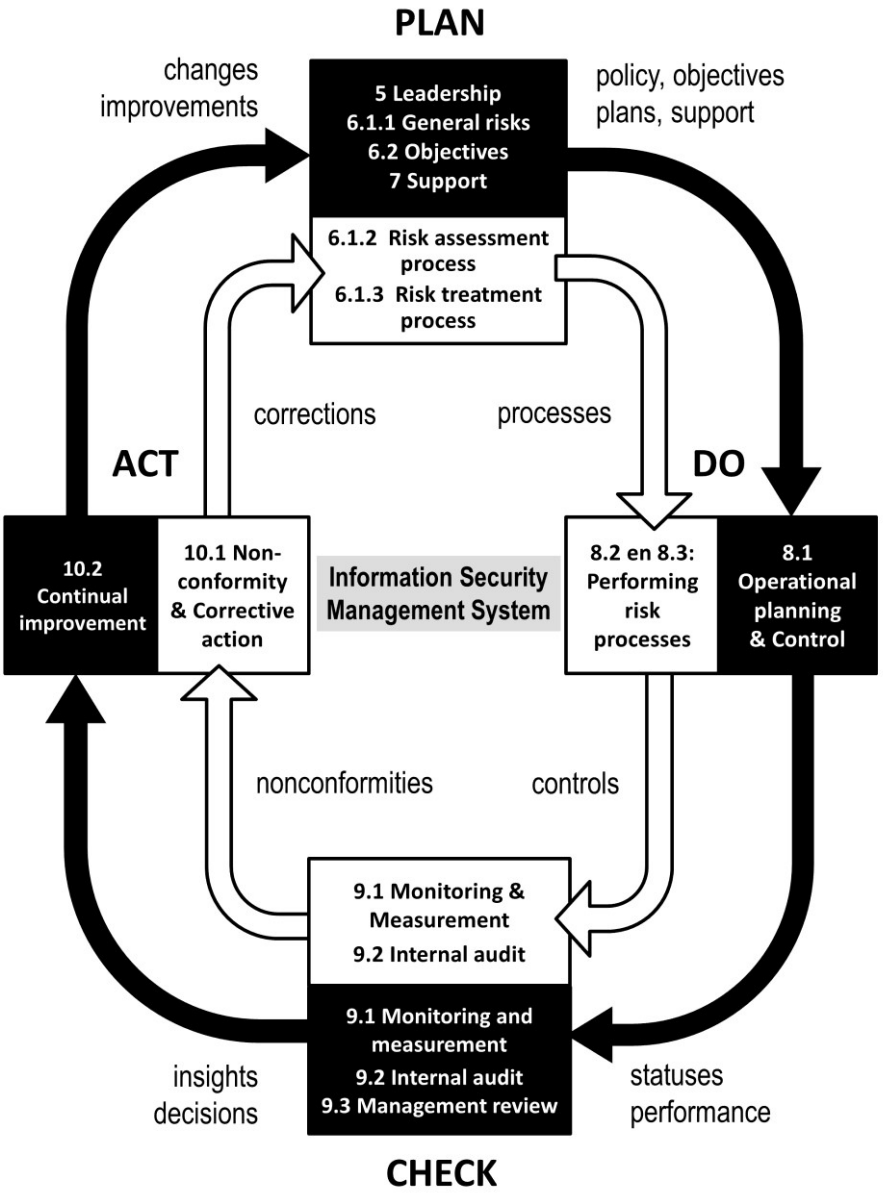
"ISMS" is a frequently used abbreviation for an *information security management system*. To avoid confusion and to remain consistent with the language use of the Standard, this book does not use the acronym ISMS.

PDCA

Although the Standard itself does not refer to the Deming quality circle, which is a globally known and widely used improvement method, the chapters of the Standard can be linked to the Plan-Do-Check-Act phases of this model.

In the image on the next page, the Standard has been translated into the Deming quality circle. The numbers and titles in the model refer to those in the Standard and this book.

The image shows a model with two PDCA circles: an inner circle (the white one) and an outer circle (the black one).


PLAN
changes
improvements
5 Leadership
6.1.1 General risks
6.2 Objectives
7 Support
policy, objectives
plans, support
6.1.2 Risk assessment process
6.1.3 Risk treatment process
corrections
processes
ACT
DO
10.2 Continual improvement
10.1 Non-conformity & Corrective action
Information Security Management System
8.2 en 8.3: Performing risk processes
8.1 Operational planning & Control
nonconformities
controls
9.1 Monitoring & Measurement
9.2 Internal audit
9.1 Monitoring and measurement
9.2 Internal audit
9.3 Management review
insights
decisions
statuses
performance
CHECK

➢ *The model of the information security management system with the two circles is from the author of this book; it does not come from the Standard.*

The inner PDCA circle of the model directly relates to the management of information security risks. This circle is already present in most organizations; there are plans for dealing with information security risks (plan), measures have been implemented to control those risks (do), checks are made as to whether the measures are effective (check) and action is taken if this is not the case (act).

Unfortunately, the inner circle does not always work well enough. As a result of a lack of discipline, and in the absence of a systematic approach, invisible dangers can creep into the organization, which suddenly strike and cause significant damage. The consequences of this can be seen daily in the form of a loss of confidentiality, integrity, and availability of information at numerous organizations.

That is why the Standard uses a second PDCA circle. This outer circle provides support to the inner circle in the form of leadership and support (plan), planning and control (do), a systematic evaluation of performance (check) and continuous improvement of the system as a whole (act). The two PDCA circles can rotate at different speeds, but the outer circle makes regular contact with the inner circle, feeds it and monitors it closely.

In this way, the implementation of an information security management system offers an improvement on two fronts: the introduction of a formal process for managing information security risks (the inner circle), and the introduction of a supporting process around it (the outer circle). The whole forms a robust system that is used throughout the world and that is still growing in popularity.

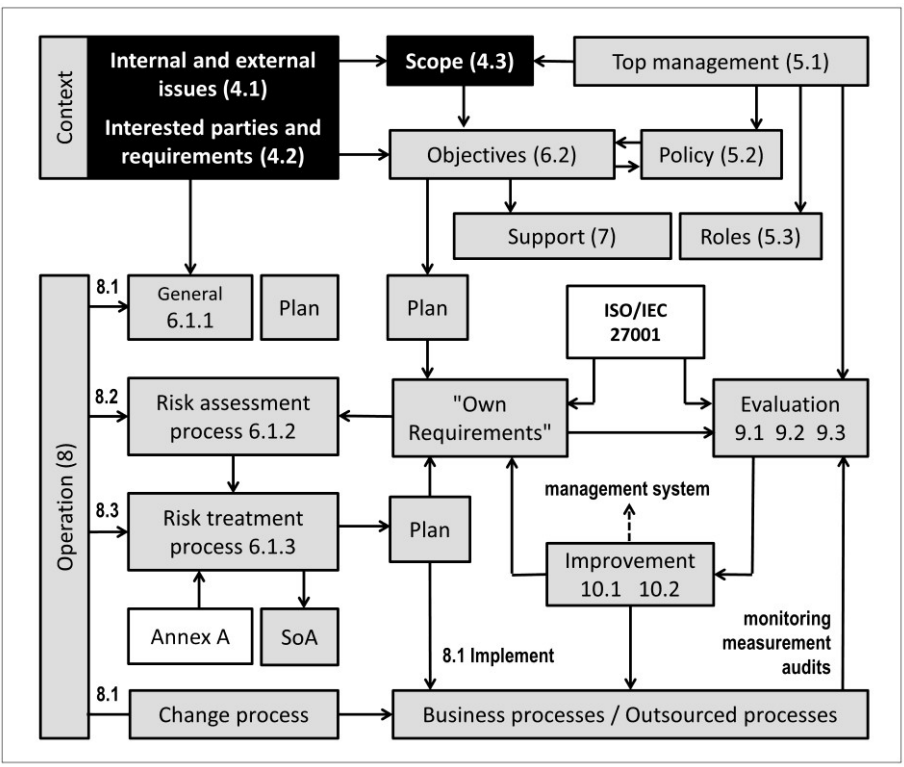
Regarding the use of the inner circle, you may need to tighten the strings a bit more tightly than you currently do, such as formally documenting and planning your processes and aligning them better with the Standard. The outer circle is still insufficiently present in many organizations, or insufficiently demonstrable.

➢ *For those who find the Deming quality circle a useful method, this book indicates to which phase of the circle the chapters belong.*

4. Context

Chapter four of the Standard deals with the following questions:

1) Which internal and external issues are relevant to your information security management system?
2) Which needs and expectations of interested parties are relevant to your information security management system?
3) What is a suitable scope for your information security management system?
4) How are you going to establish, implement, maintain and continuously improve an information security management system in accordance with the requirements of the Standard?



4.1 The organization and its context

INTRODUCTION

Clause 4.1 requires you to identify all *external and internal issues*:

- that are relevant to your *purpose*;
- that affect the ability of your organization to achieve the *intended outcome(s)* of your information security management system.

The *external and internal issues* must be used at a later stage in the implementation of your information security management system. You are expected to do this when:

- Determining the scope of your management system (see Clause 4.3);
- Determining and handling risks that prevent the information security management system from achieving its intended outcome(s) (see Clause 6.1.1);
- Establishing information security objectives [4] (see clause 6.2).

EXTERNAL AND INTERNAL ISSUES: BUSINESS OBJECTIVE

The word *purpose* mentioned in clause 4.1 refers to your business objective(s) concerning information security. For example, "providing safe and reliable services and offering our customers confidence that we manage information security risks adequately."

The question that this clause is about is, which positive and negative issues are relevant to achieving your business objective(s)?

Example

An organization's objective is, "providing safe and reliable services and offering our customers confidence that we manage information security risks adequately." During a brainstorming session, the following internal issues emerge that are relevant to this objective:

Strengths
Favorable financial position
Motivated staff
Never had serious incidents
A good level of IT knowledge
Good tools

Weaknesses
Few formal processes and rules
No internal audits
Little insight into risks
Low awareness among some employees

To get a better picture of the context, the organization includes the issues in a broader analysis by using a so-called SWOT analysis (Strength, Weakness, Opportunity, and Threat).

	ISSUES FOR ACHIEVING BUSINESS OBJECTIVES	
	POSITIVE	**NEGATIVE**
INTERNAL	**Strengths** • Favorable financial position • Motivated staff • Never had serious incidents • A lot of IT knowledge • Good tools	**Weaknesses** • Few formal processes and rules • No internal audits on the effectiveness of measures • Little insight into risks • Low awareness of information security among some employees.
EXTERNAL	**Opportunities** • An ISO/IEC 27001 certificate is an opportunity to offer customers more confidence.	**Threats** • Our problem with supplier X • Shortage in the labor market • Changing legislation • Increasingly new forms of cybercrime

➢ *Please note: the Standard does not require you to perform a SWOT analysis. To comply with Clause 4.1, you only have to identify internal and external issues.*

INTERNAL AND EXTERNAL ISSUES: ACHIEVING THE INTENDED OUTCOME

Once the strategic decision has been made to start using an information security management system, the following question arises: which positive and negative issues affect the ability of your organization to achieve the intended outcome(s) of your management system?

Example

The same organization as in the previous example also organizes a brainstorm about the internal issues that affect its ability to achieve the intended outcome of the management system. The results are used in a SWOT analysis.

INTERNAL ISSUES FOR THE MANAGEMENT SYSTEM	
POSITIVE	**NEGATIVE**
Strengths • Commitment of top management • A small organization, quick decisions • Motivated staff • A lot of IT knowledge • Good tools	**Weaknesses** • Limited workforce • Little understanding of ISO/IEC 27001 • Little knowledge of the law • Low awareness of information security among some employees • Documentation is messy
Opportunities • Reduction in the number of incidents • Improvement of existing processes • Better cooperation with customers and suppliers • Better compliance with legal and contractual requirements	**Threats** • Project X is going to require a lot of workforces this year at the expense of the management system • Three experienced employees will retire this year

It is logical that when determining internal and external issues, there is sometimes an overlap between the business objective and the intended

outcome of the management system. After all, the outcome of the management system contributes to achieving your business objective.

DETERMINING INTERNAL ISSUES

When determining internal issues, consider the size of your organization. Think of your corporate culture. Think of the maturity of leadership, policy, processes, and procedures. Think of your obligations, objectives, and plans for the future. Think of your available resources such as capital, workforce and time.

With larger organizations, other internal issues can play a role than with smaller ones. Below is an example of internal issues that could play a role in a larger organization:

Example

An organization with 150 employees and three sites sees the following internal issues that are relevant to its objective, and that can influence its ability to achieve the intended outcome of its management system:

- Top management has so far been little involved in the subject of information security.
- The three sites think differently about information security and on how to manage it.
- Decision making can be very slow.
- Activities and culture at the locations are very different.
- Seventeen employees speak a foreign language.

DETERMINING EXTERNAL ISSUES

When determining external issues, think of the influence of economic and political developments. Think of regulatory requirements in the field of information security. Think of technological developments at play outside your organization. Think of your suppliers.

The characteristic of external issues is that you usually have little or no influence on them; you must find a way to deal with them.

Pitfall 2 Issues determined for the intended scope

When determining internal and external problems, ignore the intended scope of your management system (see clause 4.3). The intention is that you determine this scope later, considering your internal and external issues.

🕮 MANDATORY DOCUMENTATION

Clause 4.1 does not require you to define or document something (words that you will find in many other clauses).

To be able to demonstrate that the requirements of the Standard are met, you can make a documented overview of your external and internal issues.

☑ INSTRUCTIONS FOR PERFORMING AUDITS

Regarding clause 4.1, an auditor could investigate:

- Whether the organization has determined a "purpose" concerning information security (this is not a requirement, but is a necessary condition according to clause 4.1);
- Whether the organization has identified internal and external issues that are relevant to its "purpose";
- Whether the organization has determined the "intended outcomes" of its information security management system (this is not a requirement, but is a necessary condition according to clause 4.1);
- Whether the organization has identified internal and external issues that may affect its ability to achieve the intended outcome(s) of its information security management system;
- Whether the organization regularly examines whether the information on internal and external issues is complete and up to date.

4.2 Interested parties

INTRODUCTION

An interested party is [1]:

- a person or organization that can affect a decision or activity of your organization;
- a person or organization that can be affected by a decision or activity of your organization;
- a person or organization who perceive themselves to be affected (positive or negative) by a decision or activity of your organization.

Clause 4.2 requires you to determine which *interested parties* are relevant to your information security management system, and which *requirements* of these interested parties are relevant to information security. The results must be used at a later stage in the implementation of your information security management system. As with the internal and external issues (see clause 4.1) you are expected to do this when:

- determining the scope of your management system (see clause 4.3);
- determining and handling risks that prevent the information security management system from achieving its intended outcome(s) (see clause 6.1.1);
- establishing information security objectives [4] (see clause 6.2).

INTERESTED PARTIES: TYPES OF INTERESTED PARTIES

The following types of interested parties can be distinguished:

- *Internal*: persons or parties within your organization.
- *External*: external persons or organizations such as customers, partners, suppliers, and creditors.
- *Interface*: parties that are not involved in the organization but have a specific (legitimate) interest and exert influence. Think of the government, regulators, chamber of commerce, sector organizations, society, etc.

◆ INTERESTED PARTIES

Below are some examples of interested parties that may influence or are influenced by your organization.

INTERESTED PARTIES (INTERNAL): TOP MANAGEMENT

Top management is the first relevant, interested party for the information security management system. Top management has every interest in ensuring that the business objective is not compromised and that the management system achieves its intended outcomes. If it is up to the Standard, then top management plays a crucial role in information security (see clauses 5.1, 5.2, 5.3 and 9.3).

INTERESTED PARTIES (INTERNAL): EMPLOYEES

Your employees are also a very relevant interested party for the information security management system. Employees need guidance, training, and resources to perform tasks correctly and timely. Besides, employees expect their personal data to be stored securely and not to be shared with anyone.

INTERESTED PARTIES (EXTERNAL): CUSTOMERS

What do your customers expect when it comes to information security? That depends on what you do. Do you develop software? Then your customers expect that the software is well-protected. Do you provide hosting services? Then your customers probably require that your services have a certain degree of availability. Do you offer data center services? Then you promise your customers a safe and stable environment for their IT systems. Do you have a printing office? Then the printing of your customers may not be viewed by everyone. Do you work with personal data? Then those data must be protected according to the law.

Usually, your customers have a simple reason to set information security requirements, namely that their reputation or even their survival may be at stake the moment you do foolish things. Another possibility is that a customer has certain contractual obligations to his clients and that he has to

transfer part of it to you. And when it comes to the processing of personal data, for most countries, there is also legislation.

- *For EU countries: The General Data Protection Regulation (GDPR) states in article 28 paragraph 3 [10]: "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller (…)."*

The higher the information security risks, the more your customers will insist on making agreements. Ultimately, all agreements about information security will, directly or indirectly, be traceable to preserving the availability, integrity, and confidentiality of information (see chapter 1 of this book). Nowadays, customers are increasingly demanding an ISO/IEC 27001 certificate from their suppliers.

INTERESTED PARTIES (EXTERNAL): CONSUMERS

The activities and decisions of your organization may have a direct impact on consumers who use your products or services. Consumers have rights. You are probably already familiar with the existence of legal requirements about the protection of personal data (a particular form of information).

INTERESTED PARTIES (EXTERNAL): SUPPLIERS

Suppliers can be very relevant to the information security management system, especially suppliers to whom you have outsourced key processes (see clause 8.1 on determining and controlling outsourced processes).

Most suppliers will do their best to give you confidence that they manage their information security risks adequately, for example, by providing reports on service levels, vulnerability studies, and disruptions. Suppliers are increasingly choosing to prove their information security competence by obtaining an ISO/IEC 27001 certificate, or have customers insisting on this.

INTERESTED PARTIES (INTERFACE): CENTRAL GOVERNMENT

The central government is another interested party. Everywhere in the world, IT infrastructure and systems play an essential role in the functioning