ISO 27001 RISK MANAGEMENT IN PLAIN ENGLISH

ISO POCKET BOOK SERIES

01

A Step-by-Step Handbook for
Information Security Practitioners in Small Businesses

DEJAN KOSUTIC

ISO 27001

Risk Management in Plain English

Also by Dejan Kosutic:

Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own

9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual

Becoming Resilient: The Definitive Guide to ISO 22301 Implementation

Dejan Kosutic

ISO 27001 Risk Management in Plain English

Step-by-step handbook for information security practitioners in small businesses

Advisera Expert Solutions Ltd
Zagreb, Croatia

Limit of Liability / Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. This book does not contain all information available on the subject. This book has not been created to be specific to any individual's or organization's situation or needs. You should consult with a professional where appropriate. The author and publisher shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have been incurred, directly or indirectly, by the information contained in this book.

First published by Advisera Expert Solutions Ltd
Zavizanska 12, 10000 Zagreb
Croatia
European Union
http://advisera.com/

ISBN: 978-953-57452-8-0

First Edition, 2016

ABOUT THE AUTHOR

Dejan Kosutic is the author of numerous articles, video tutorials, documentation templates, webinars, and courses about information security and business continuity management. He is the author of the leading ISO 27001 & ISO 22301 Blog, and has helped various organizations including financial institutions, government agencies, and IT companies implement information security management according to these standards.

Click here to see his LinkedIn profile

TABLE OF CONTENTS

LIST OF FIGURES

PREFACE

When my book *Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own* was published earlier this year, I soon realized that many people were reading it primarily because they wanted to learn how to perform risk assessment and treatment in their companies.

Therefore, I have created this shorter book, a part of the handbook series, which is focused solely on the issues of risk management according to ISO 27001. This book, *ISO 27001 Risk Management in Plain English,* is actually an excerpt from *Secure & Simple*, and has been edited with only a few smaller details. So, if you compare the sections from *Secure & Simple* that speak about risk management, you'll see the same sections here, with basically the same text.

So, why have another book with almost the same text? Because I wanted to provide a quick read for people who are focused solely on risk management, and don't have the time (or need) to read a comprehensive book about ISO 27001, i.e., a book like *Secure & Simple*.

Another benefit is that this book has all the sections about risk management placed in sequential, continuous form, whereas in *Secure & Simple,* the risk assessment and treatment sections are scattered throughout a couple of chapters.

You might also be puzzled by the fact that this book is rather short, whereas there are other books on ISO 27001 risk management on the market that are much more lengthy and detailed. Is it really possible to explain such a complex subject in a short book like this? Well, there are two answers for this:

First, this book is focused on implementing risk management in smaller companies – therefore, I have intentionally simplified the methodology so that it can be easily implemented, and left out all the elements that would be needed only for larger companies.

Second, and more importantly, I followed my company mission: "We make complex frameworks easy to understand and simple to use." In other words, it is easy to complicate things, but it is difficult to make things easy to understand. So, when you start reading this book you'll notice I eliminated all the hard-to-understand talk, all the unnecessary details, and focused on what exactly needs to be done, in a language understandable for beginners with no prior experience in risk management.

So, rest assured: if you are a smaller organization, by using this book you will be able to implement risk assessment and treatment in your company in a rather quick way, fully compliant with ISO 27001 and acceptable for the certification audit. And, perhaps most importantly: you will see real benefits of performing risk management in your daily business operations

1
INTRODUCTION

Why would your company need to perform risk assessment and treatment? How is this related to safeguards? Why does risk management have central place in ISO 27001?

And, is this book the right choice for you?

1.1 Who should read this book?

This book is written primarily for beginners in this field and for people with moderate knowledge about risk assessment and treatment – I structured this book in such a way that someone with no prior experience or knowledge about information security can quickly understand what it is all about, and how to implement the whole risk management project; however, if you do have experience with ISO 27001, but feel that you still have gaps in your knowledge, you'll also find this book very helpful.

This book provides examples of implementing the standard in smaller and medium-sized organizations (i.e., companies with up to 500 employees). All the principles described here are also applicable to larger organizations, so if you work for a larger company you might find this book useful; however, please be aware that you will have to use more complex methodology – for example, when performing risk assessment for a large company, you'll notice that a scale for assessing the likelihood of 3 levels will probably not be enough, so you'll have to use a scale of 5 levels.

So, if you are an IT administrator, information security professional, head of an IT department, or a project manager tasked with implementing risk management in a small or mid-sized company, this book is perfect for you.

I think this book will be quite useful for consultants, also – being a consultant myself I made an effort to present in this book the most logical way to implement risk management, so by carefully reading this book you will gain the know-how for your future consulting engagements.

Finally, I think this book can be a kind of checklist for experienced information security practitioners – I'm saying this because I've had many such experienced professionals in my risk management courses, and although they didn't learn anything especially new, they were thankful for getting a comprehensive and structured view of how information security risks should be handled.

And, this is exactly how this book is written – it gives a systematic picture of what ISO 27001 risk management is all about, and how to make sure you didn’t forget something. It doesn’t really matter whether your company will go for the certification or not – this book will explain how to use risk management within ISO 27001 framework, and to become fully compliant with this standard.

1.2 How to read this book?

This book is written as a step-by-step implementation guide for risk management, and you should read the Chapter Steps in the risk management in the exact order as it is written, because this sequence represents the most optimal way of implementing the risk management according to ISO 27001.

Here are also some other features of this book that will make it easier for you to read it and use it in practice.

- When certain sections of this book are related to a particular clause in the standard, then the clause from ISO 27001 is written in the title of that section.
- Since Chapter 2 describes the implementation of particular clauses of the standard, each section has these elements:
    - **Purpose** – describes briefly why such a clause exists and how it can be used for your risk management
    - **Inputs** – which inputs you need to have in order to implement the requirement
    - **Options** – which options you should consider when implementing the requirement
    - **Decisions** – which decisions you need to make to move forward
    - **Documentation** – describes how to document the requirements of ISO 27001
    - **Documentation tip** – briefly summarizes the documents you need for each requirement
- Some sections contain tips for free tools, which will enable you to implement the standard in an easier way.
- At the end of Chapter 2 you'll see a section called "Success factor" which will emphasize what you need to focus on.
- At the end of the book, in chapter 3 you'll see a shorter case study which explains how risk management is implemented in real situation.
- You'll find useful list of threats and vulnerabilities in the appendix of this book.

1.3 What this book is not

This book is focused on how to manage risk assessment and treatment, but it is not focused on technology. This book won't explain what backup system you need to purchase, but this book will give you a methodology on how to get all the inputs so that you can make relevant technology decisions – e.g. how to determine which sensitive data you have and how often it needs to be backed up.

This book won't give you finished templates for all your policies, procedures, and plans; however, this book will explain to you how to structure every document required for risk management by ISO 27001, which options you have for writing such documents, who should be involved in writing and decision making related to each document, where to find the inputs, etc.

This book is not a copy of ISO 27001 and ISO 27005 standards – you cannot replace reading the standard by reading this book. This book is intended to explain how to interpret the standards (since the standards are written in a rather unfriendly way), and how to implement every element of the standard using best practices based on experience; however, this book is not a replacement for ISO 27001 nor ISO 27005.

So, please don't make the mistake of starting an implementation without actually reading at least ISO 27001, and potentially also ISO 27005 – I think you'll find ISO 27001 and ISO 27005 together with this book to be the perfect combination for your future work.

1.4 Why is risk management the central philosophy in ISO 27001?

When speaking with someone new to ISO 27001, very often I encounter the same problem: this person thinks the standard will describe in detail everything they need to do – for example, how often they will need to perform backup, how distant their disaster recovery site should be, or even worse, which kind of technology they must use for network protection or how they have to configure the router.

But, the fact is ISO 27001 does not prescribe these things; it works in a completely different way.

Why is ISO 27001 not prescriptive? Let's imagine that the standard prescribes that you need to perform a backup every 24 hours – is this the right measure for you? It might be, but believe me, many companies nowadays will find this insufficient – the rate of change of their data is so quick that they need to do backup if not in real time, then at least every hour. On the other hand, there are still some companies that would find the once-a-day backup too often – their rate of change is still very slow, so performing backup so often would be overkill.

The point is – if this standard is to fit any type of a company, then this prescriptive approach is not possible. So, it is simply impossible not only to define the backup frequency, but also which technology to use, how to configure each device, etc.

By the way, this perception that ISO 27001 will prescribe everything is the biggest generator of myths about ISO 27001 – you'll find these myths in the next section.

So, you might wonder, "Why would I need a standard that doesn't tell me anything concretely?" Because ISO 27001 gives you a framework for you to decide on appropriate protection. The same way, e.g., you cannot copy a marketing campaign of another company to your own, this same principle is valid for information security – you need to tailor it to your specific needs.

Risk management is the central idea of ISO 27001. And, the way ISO 27001 tells you to achieve this tailor-made suit is to perform risk assessment and risk treatment. This is nothing but a systematic overview of the bad things that can happen to you (assessing the risks), and then deciding which safeguards to implement to prevent those bad things from happening (treating the risks).

Requirements of interested parties. These requirements are a second crucial input when selecting the safeguards. Interested parties could be government agencies, your clients, partners, etc. – all of them probably expect you to protect the information, and this is reflected in the laws and contracts you have with them. Therefore, your safeguards have to comply with all these requirements as well.

The whole idea here is that you should implement only those safeguards (controls) that are required because of the risks and requirements of interested parties, not those that someone thinks are fancy; but, this logic also means that you should implement all the controls that are required because of the risks or because of these requirements, and that you cannot exclude some simply because you don't like them.

IT alone is not enough to protect the information. If you work in the IT department, you are probably aware that most of the incidents are happening not because the computers broke down, but because the users from the business side of the organization are using the information systems in the wrong way.

And, such wrongdoings cannot be prevented with technical safeguards only – what is also needed are clear policies and procedures, training and awareness, legal protection, discipline measures, etc. Real-life experience has proven that the more diverse safeguards are applied, the higher level of security is achieved.

And, when you take into account that not all the sensitive information is in digital form (you probably still have papers with confidential information on them), the conclusion is that IT safeguards are not enough, and that the IT department, although very important in an information security project, cannot run this kind of project alone.

This fact that IT security is not enough for implementing information security is recognized in ISO 27001 – this standard tells you how to run the information security implementation as a company-wide project where not only IT, but also the business side of the organization, must take part.

1.5 Relationship between enterprise risk management and information security management

Essentially, information security is part of overall (i.e. enterprise) risk management in a company, with areas that overlap with cybersecurity, business continuity management, and IT management.

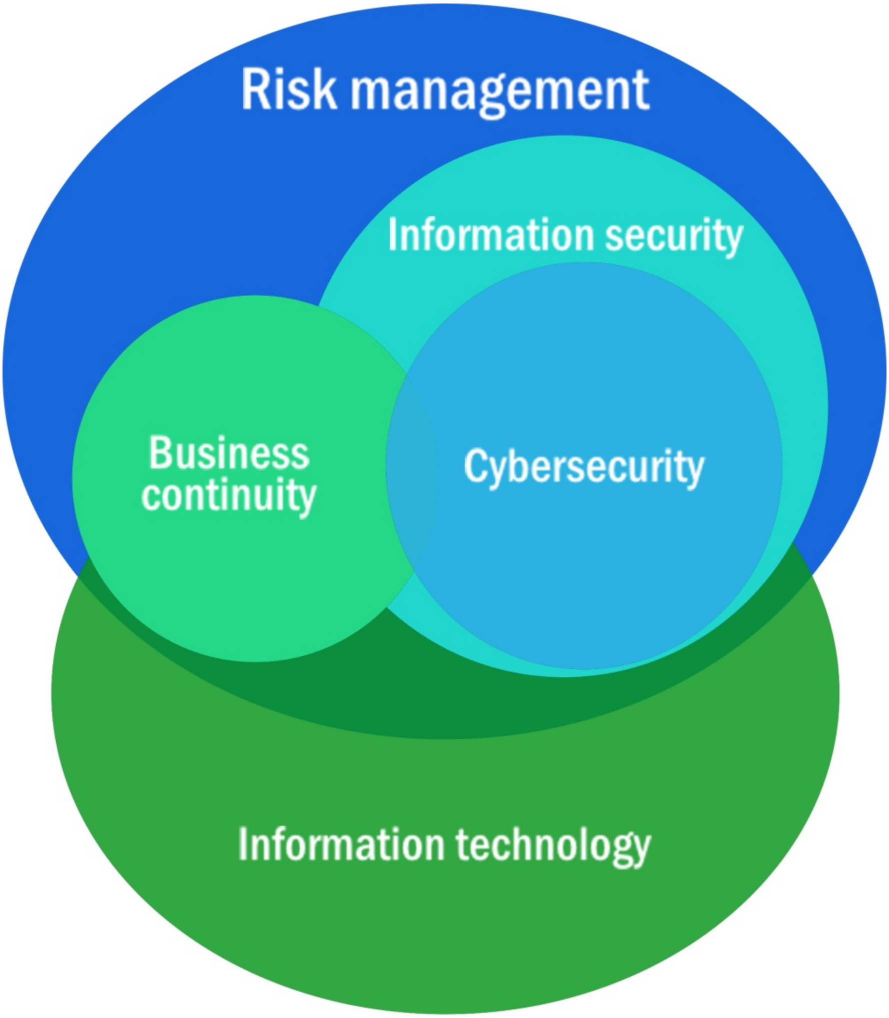

Figure 1: Relationship between enterprise risk management, information security, business continuity, IT, and cybersecurity

Cybersecurity is basically a subset of information security because it focuses on protecting the information in digital form, while information security is a slightly wider concept because it protects the information in any media. The overlap with business continuity exists because its purpose is to enable the availability of information, which is also one of the key roles of information security. Naturally, information technology plays an extremely important role in information security; so, consequently, there is also an overlapping area.

But, the most important thing is that information security, cybersecurity, and business continuity have the same goal: to decrease the risks to business operations. You may not call it risk management in your day-to-day job, but basically this is what information security does – assess which potential problems can occur, and then apply various safeguards or controls to decrease those risks.

Some industries have formally recognized information security as part of risk management – e.g., in the banking world, information security belongs very often to operational risk management. My guess is that in the future we will see more and more information security professionals work in the risk management part of their organizations, and information security will tend to merge with business continuity.

1.6 ISO 27001 vs. ISO 27005 vs. ISO 31000

ISO 31000 provides guidelines on how to organize risk management in organizations – this standard is not focused solely on information security risks; it can be used for any type of risks including business continuity, market, currency, credit, operational, and others.

It provides a detailed glossary of risk management terms, explains basic principles of risk management, and provides a general framework including a PDCA cycle for risk management. However, being applicable to any type of organization and to any type of risk, it does not provide specific methodology for, e.g., information security risk management.

Relationship between ISO 31000 and ISO 27001. The previous 2005 revision of ISO 27001 did not mention ISO 31000, but the new 2013 revision does, and this has caused confusion – many people think they have to implement something new in ISO 27001 because of ISO 31000, but this is not true.

This is what ISO 27001 says about ISO 31000: In clause 4.1, ISO 27001 notes that you could consider the external and internal contexts of the organization according to clause 5.3 of ISO 31000. And, indeed, clauses 5.3.2 and 5.3.3 of ISO 31000 are quite useful in that respect because they provide valuable guidelines on internal and external contexts; however, ISO 27001 mentions ISO 31000 only in a note, which means these guidelines are not mandatory.

In clause 6.1.3, ISO 27001 notes that information security management in ISO 27001 is aligned with ISO 31000. Therefore, ISO 27001 does not say you need to implement risk assessment and treatment according to ISO 31000 – it only says that all the requirements from ISO 27001 are already compliant with ISO 31000. Therefore, you can implement risk management in any way you wish, as long as it is compliant with ISO 27001.

ISO 31000 vs. ISO 27005. As mentioned before, ISO 31000 does not offer any specific advice about information security risk assessment and risk treatment; for that purpose, ISO 27005 – a standard that gives guidelines for information security risk assessment and treatment – is much better. It gives you the know-how to identify assets, threats, and vulnerabilities, to assess consequences and probability, to calculate risk, etc. And, it is completely compliant with ISO 31000.

So, why would you use ISO 31000? Besides those already-mentioned guidelines for identifying internal and external contexts, its biggest value is in providing a framework for managing all kinds of risks on a company-wide level – it can help you turn risk management from some obscure, hard-to-understand issue into a mindset that is easily understood by everyone in the company.

Since ISO 31000 describes how to approach risk management strategically and comprehensively, you can consider this standard to be an excellent framework for Enterprise Risk Management (ERM). So, once you master your information security risk management, you can use it as a foundation for building the ERM, although doing it the other way around might be better in theory

1.7 Additional resources

Here are some resources that will help you, together with this book, to learn about ISO 27001 risk management and how to implement it:

- **ISO 27001 online courses** – free online courses that will teach you the basics of risk management in ISO 27001
- **ISO 27001 free downloads** – collection of white papers, checklists, diagrams, templates, etc.
- **ISO 27001 tools** – couple of free tools like Return on Security Investment Calculator, Implementation Duration Calculator, and Gap Analysis Tool.
- **ISO 27001 Risk Assessment Toolkit** – set of all the documentation templates that are required by ISO 27001 for risk management, with included expert support for the implementation.

- **Expert Advice Community** – a forum where you can ask a question on risk management (or any other ISO-related topic) and get the answers from leading experts
- **Official ISO webpage about ISO 27001** – here you can purchase an official version of ISO 27001 and ISO 27005.

2
STEPS IN THE RISK MANAGEMENT

Risk assessment and treatment are certainly the most complex parts of ISO 27001 implementation, but you cannot afford to avoid them – without these steps you wouldn't know where to focus your information security efforts, which means you would miss something important.

Luckily, this process can be quite streamlined – if you don't complicate it with unnecessary elements, it can be finished in a pretty acceptable time and with reasonable effort. What's more, you'll be quite surprised at what you learned about your company in this process.

2.1 Addressing risks and opportunities (clause 6.1.1)

In addition to the analysis of context of the organization and the interested parties (clauses 4.1 and 4.2 of ISO 27001), in the process of planning the ISMS companies should identify the risks and opportunities that need to be addressed. This is the only way to prevent incidents from happening, while at the same time achieving other objectives of the ISMS. By the way, addressing risks and opportunities has taken over the role of preventive actions that existed in the old 2005 revision of ISO 27001.

Risks refer to unwanted events that can have negative impact on the information security, and hence, to the company, such as a flood that might destroy paper-based information. Opportunities refer to the actions that the company could undertake in order to improve the information security, such as hiring a trained information security expert, like a CISO (Chief Information Security Officer), who would do a better job than someone who has no skills; opportunities might also mean increasing the risks if this makes business sense – for example, a decade ago most of the banks introduced Internet banking, although that meant increasing the security risks.

I'll explain how to address risks in the following sections; on the other hand, addressing opportunities can be integrated into the continual improvement process, which means opportunities can be documented and evaluated as the initiatives for continual improvement of the ISMS – in such case you should do the following:

- Define who is responsible for planning, managing, and coordinating improvement activities.
- Communicate that all employees can contribute to continual improvement of the ISMS.
- Define ways to record all relevant information related to improvements.
- Implement the improvement as a change by documenting the changes, the rationale behind them, and the expected outcome, as well as reviewing the effectiveness of the changes.

Addressing opportunities can also be part of setting the security objectives and measuring their fulfillment. For example, if the company decides to choose one of its employees to be the CISO, there would be opportunities for this person to enhance his/her information security knowledge. For that purpose, the company can initiate action for improvement of this person's knowledge and can set an objective for the CISO to obtain appropriate security certificates.

BIBLIOGRAPHY

ISO 22301: 2012, Societal security – Business continuity management systems – Requirements

ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management

ISO 31000:2009, Risk management – Principles and guidelines

SP800 series, NIST

Kosutic, Dejan, *9 Steps to Cybersecurity*, Zagreb: EPPS Services Ltd, 2012

Kosutic, Dejan, *Becoming Resilient*, Zagreb: EPPS Services Ltd, 2013

Kosutic, Dejan, *Secure & Simple*, Zagreb: EPPS Services Ltd, 2016

http://advisera.com/27001academy/blog/ *ISO 27001 & ISO 22301 Blog*, Advisera.com

http://training.advisera.com/course/iso-27001-foundations-course/ *ISO 27001 Foundations Course*, Advisera.com

INDEX

ISO 27001 Risk Management in Plain English

Step-by-step handbook for information security practitioners in small businesses

Think and act like a consultant with this comprehensive, practical, and step-by-step guide to implementing risk management compliant with ISO 27001.

Author and experienced information security consultant Dejan Kosutic shares all his knowledge and practical wisdom with you in one invaluable book.

- ✓ Get a simple explanation of what ISO 27001 requires of risk assessment and treatment.
- ✓ Learn what are the steps in risk management.
- ✓ Learn how to develop the risk assessment and treatment methodology
- ✓ Learn which options exist for risk management according to ISO 27001
- ✓ Learn which documents are required for risk management.
- ✓ All this, and much more…

Written in plain English and leaving the technical jargon to the geeks, *ISO 27001 Risk Management in Plain English* is written for normal people in plain, simple language. Whether you're an information security practitioner or new to the field, it's the only book you'll ever need on the subject.