SECURE & SIMPLE

A Small-Business Guide To Implementing ISO 27001 On Your Own

THE PLAIN ENGLISH, STEP-BY-STEP HANDBOOK FOR INFORMATION SECURITY PRACTITIONERS

DEJAN KOSUTIC

Dejan Kosutic

Secure & Simple:

A Small-Business Guide to Implementing ISO 27001 On Your Own

The plain English, step-by-step handbook for information security practitioners

EPPS Services 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 EPPS Services Ltd
Zavizanska 12, 10000 Zagreb
Croatia
European Union
http://advisera.com/

ISBN: 978-953-57452-5-9 (eBook)
ISBN: 978-953-57452-6-6 (printed book)

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

I see thousands of visitors daily reading my articles in ISO 27001 Blog, and although many people are thanking me for them, some of them are complaining a little bit – they say, "Yes, your articles are useful, but there are so many of them, I simply don't know where to start and where to end." And, indeed – at the time of writing this book, there were almost 200 articles published on 27001Academy, so they are right – it is hard to use all that knowledge in a systematic way.

This is why I decided to write this book – I wanted to provide a comprehensive, step-by-step guide for ISO 27001, written in a simple language that can be understood by beginners with no prior knowledge of this standard, written in a structured way so that you know where to begin and how to end your ISO 27001 implementation in a successful way.

And, yes, I admit – lots of content in this book is taken from the most popular articles on the website, from my book Becoming Resilient, from our online courses, and other materials, because I thought a book that would present all those materials in such a structured way would provide a good value.

But, what I think you'll like the most about this book is that I give practical answers to real-life situations when implementing ISO 27001. These bits of advice came primarily from my interaction with many people who are asking me questions on a daily basis – I was lucky enough to be in a position to deliver many in-person courses and online webinars, answer thousands of questions through forums, deliver many consulting jobs, and speak at a number of conferences. On all of these occasions, I was forced to think through many issues surrounding ISO 27001, and to provide the best practice on how to handle them.

Therefore, after reading this book, you'll be able to implement the standard yourself, since it will provide you with enough knowledge and tips to implement the standard in a small or mid-sized company.

Hope I succeeded in this. Enjoy your book!

1
INTRODUCTION

Why would your company need to keep its information safe? How can ISO 27001 help you achieve information security? And, is this book the right choice for you?

1.1 Why information security? Why ISO 27001?

Information security, cybersecurity, or data protection are not the things that are reserved any more for IT geeks only – this is something that concerns virtually any person on this planet, as well as any company.

If you were an executive in an organization 10 years ago, you probably would not be so concerned with any of these things. Today, you are in the second decade of the third millennium and you cannot ignore threats to your data anymore. What's more, in the future you will need even more protection. Why? Because the majority of organizations are now in the business of processing information.

Most of us imagine that a bank handles large amounts of cash every day. While the banks still conduct many cash transactions, the fact is electronic money transactions far outweigh cash transactions – in some cases by more than a million to one. So, this means that a typical bank is in the business of processing information – it is one large factory of information. And, guess what: For some time now, robbing a bank by hacking is far more profitable than walking in with a mask over your face and robbing the tellers. And, hacking is far less risky, too.

Think about your business; are you an information factory, too? Chances are, your business is, if not completely, then in most part about processing information. This means your business is more vulnerable. Your information, your knowledge, your know-how, and your intellectual property are all at risk. And now the one-million-dollar question, or if you are in a larger business this might be a one-billion-dollar question: What do you need to do to protect the information in your company, and where do you start?

The problem nowadays is there is an abundance of information about information security; you are probably bombarded with information about new firewalls, anti-virus software, frameworks, methodologies, legislation, and so on. Many companies offer services claimed to be the solution to all of your security problems. Yet, these individual solutions aren't going to protect you completely. For instance, you cannot solve the problem of a disgruntled employee with a firewall, the same way you cannot solve the problem of a hacker just by complying with a law.

So, it's obvious you need something more, something comprehensive. But, the challenge is where to even begin, what steps to take that will best protect your business.

This is where ISO 27001 comes in – as explained throughout this book, it provides a comprehensive framework that will help you with this crucial process. It gives you the necessary guidance and building blocks for protecting your company. ISO 27001 tells you where to start from, how to run your project, how to adapt the security to the specifics of your company, how to control what the IT and security experts are doing, and much more.

So, the point is – ISO 27001 doesn’t have to be just another bureaucratic compliance job – if implemented properly, it can be a very efficient tool not only to protect your company, but also to achieve some business benefits.

1.2 Basic information security principles

First, let us define what information is. Information is an asset of the organization, which has value to the organization and needs to be protected appropriately. Information can have various forms and can be stored on different media.

On the other hand, information security can be defined as protecting the confidentiality, integrity, and availability of information in various forms, such as written, spoken, printed, electronic, and so on.

Let's see the official definitions of these terms from ISO 27000: confidentiality is "property that information is not made available or disclosed to unauthorized individuals, entities, or processes," integrity is "property of accuracy and completeness," and availability is "property of being accessible and usable upon demand by an authorized entity."

Yes, sometimes it is difficult to understand this ISO terminology, so here is an easy explanation of these basic concepts: if I come to a bank and deposit $10,000, first of all I do not want anyone else to know about this money except for the bank and myself. (This is confidentiality.)

In a few months' time when I come to withdraw my deposit, I want the amount to be $10,000 plus any interest; I do not want the amount to be $1000 because someone has played around with my account. (This is integrity.)

Lastly, when I want to withdraw my money I do not want the bank clerk to tell me that the bank's systems are down and that I have to come back tomorrow. (This is availability.)

ISO 27001 has exactly the same focus – protection of confidentiality, integrity, and availability (also known as the C-I-A triad); but, it also goes a step further – it explains how to do it systematically in a company of any type.

1.3 ISO 27001 puts it all together

What I like about ISO 27001 is that it has this comprehensive, and at the same time, balanced approach to building up an information security management system (ISMS) – it not only gives a perfect balance between the IT and business sides of the organization, it also requires the direct involvement of top management in the information security implementation, ensuring that such project not only has all the required resources, but that it also supports the strategic objectives of the company.

ISO 27001 explains how to structure the information security documentation, but also how to apply only those security controls (safeguards) that are really necessary for the company. It gives you the tools to permanently review the whole system and improve it whenever it is possible; it provides you with a system on how to train your employees and make them aware of the importance of information security; it includes the requirements on how to plan the resources, including financial resources.

As I will explain later on in greater detail, it gives a perfect implementation path – it is written in such a sequential way that you just have to follow the structure of the standard to implement your ISMS in the most logical way.

Finally, it provides a management framework on how to evaluate whether information security has achieved some business value – by setting objectives and measuring whether these objectives are fulfilled. You may be surprised, but I like this part very much – this is because if the management sees concrete benefits from their information security investment, it is the best way to ensure the long and successful life of the ISMS in your company.

1.4 Who should read this book?

This book is written primarily for beginners in this field and for people with moderate knowledge about ISO 27001 – 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 project; however, if you do have experience with the standard, 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 in some cases the solutions will have to be more complex than the ones described in this book – for example, you might want to use a more complex risk assessment methodology than the one that is suggested in Chapter 7 Risk management.

So, if you are an IT administrator, information security professional, head of an IT department, or a project manager tasked with implementing ISO 27001 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 an Information Security Management System (ISMS), so by carefully reading this book you will gain the know-how for your future consulting engagements.

This book is not written as a guide for performing the audits, but it might be useful for internal auditors, or even certification auditors, because it will help them understand all the requirements of the standard, and it will also present the best practice for the implementation – this will be useful when the auditor needs to provide some recommendations in his or her audit report.

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 ISO 27001 courses, and although they didn't learn anything especially new, they were thankful for getting a comprehensive and structured view of how information security should be implemented.

And, this is exactly how this book is written – it gives a systematic picture of what ISO 27001 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 ISO 27001 as a framework, and to become fully compliant with this standard.

1.5 How to read this book

This book is written as a step-by-step implementation guide, and the way is to read Chapters 3 to 11 in the exact order as they are written, because this sequence represents the most optimal way of implementing the standard.

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 standard clause is written in the title of that section.

- Since Chapters 5 to 8 and 10 describe 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 ISMS

  - **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 – for example, in section 3.3 that speaks about convincing your top management, you'll find a link to a Return on Security Investment Calculator.

- At the end of most important chapters you'll see a section called "Success factors," which will emphasize what you need to focus on.

- At the end of the book, in chapter 14 you'll see a couple of shorter case studies which explain how particular elements of ISO 27001 are implemented in real situations.

- You'll find lots of useful information in the appendices – glossary, implementation diagram, checklist of mandatory documentation, comparison matrices, templates for project planning, etc.

1.6 What this book is not

This book is focused on managing security, project management, documentation, how to get the support for your project, etc., but it is not focused on technology. This book won't explain which kind of backup systems you need to purchase, which communication technology you should use, or which kind of firewall you should install. However, this book will give you a methodology on how to get all the inputs so that you can make relevant technology decisions – how to determine which sensitive data you have together with your colleagues from the business side and how to make sure it is backed up regularly, what information you need to communicate and to whom, what are the threats to your systems that your firewall should protect you against, etc.

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 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 the ISO 27001 standard – you cannot replace reading the standard by reading this book. This book is intended to explain how to interpret the standard (since the standard is 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 itself.

So, please don't make the mistake of starting an implementation of a standard without actually reading it – I think you'll find the ISO 27001 standard and this book to be the perfect combination for your future work. You can purchase the standard at the **ISO official website;** there is also a cheaper alternative at the **ANSI website.**

1.7 Additional resources

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

1) **ISO 27001 online courses** – free online courses that will teach you the basics of ISO 27001, how to implement the standard, how to perform an audit, etc.

2) **ISO 27001 free downloads** – collection of white papers, checklists, diagrams, templates, etc.

3) **ISO 27001 tools** – couple of free tools like Return on Security Investment Calculator, Implementation Duration Calculator, and Gap Analysis Tool.

4) **Conformio** – cloud-based document management system (DMS) and project management tool focused on ISO standards.

5) **ISO 27001 Documentation Toolkit** – set of all the documentation templates that are required by ISO 27001, with included expert support for the implementation.

6) **Official ISO webpage about ISO 27001** – here you can purchase an official version of the ISO 27001 standard.

Got you interested? Fine, let's see more closely what ISO 27001 is all about.

7
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.

7.1 Addressing risks and opportunities (clause 6.1.1)

In addition to the previously mentioned analysis of context of the organization and the interested parties, 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, 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, as I'll describe in section 10.6; 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.

7.2 Five steps in the risk management process (clause 6.1)

Risk assessment and treatment (together they are called *risk management*) are the most important steps at the beginning of your information security project – they set the foundation for information security in your company.

The question is – why are they so important? The answer is quite simple, although not understood by many people: the main philosophy of ISO 27001 is to find out which incidents could occur (i.e., assess the risks) and then find the most appropriate ways to avoid such incidents (i.e., treat the risks). Not only this, you also have to assess the importance of each risk so that you can focus on the most important ones.

Although risk management is a complex job, it is very often unnecessarily mystified. These five basic steps will shed light on what you have to do:

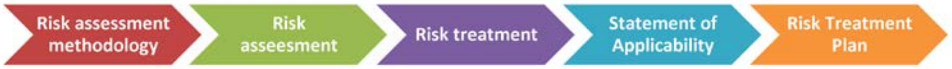

Figure 5: Five steps in the risk management process

1) Risk assessment methodology. This is the first step on your voyage through risk management. You need to define rules on how you are going to perform the risk assessment and treatment, because you want your whole organization to do them the same way – the biggest problem with risk management happens if different parts of the organization perform it in a different way. Therefore, you need to define which scales you will use for qualitative assessment, what will be the acceptable level of risk, etc.

2) Risk assessment implementation. Once you know the rules, you can start finding out which potential problems could happen to you – usually you will list all your assets, then threats and vulnerabilities related to those assets, assess the impact and likelihood for each combination of assets/threats/vulnerabilities, and finally, calculate the level of risk.

3) Risk treatment implementation. Of course, not all risks are created equal – you have to focus on the most important ones, so-called "unacceptable risks." There are four options you can choose from to mitigate each unacceptable risk: apply security controls, transfer the risk, avoid the risk, and accept the risk.

4) Statement of Applicability. This document actually shows the security profile of your company – based on the results of the risk treatment you need to list all the controls you have implemented, why you have implemented them, and how. This document is also very important because the certification auditor will use it as the main guideline for the audit.

5) Risk Treatment Plan. The purpose of this document is to define exactly who is going to implement each control, in which timeframe, with which budget, etc. I would prefer to call this document "Implementation Plan" or "Action Plan," but let's stick to the terminology used in ISO 27001.

As you'll see in further sections, this process is quite straightforward, and actually not as difficult as it might have seemed at the beginning. The good thing is – ISO 27001 forces you to perform this whole risk management in a systematic way.

It is very important to understand that these five steps need to be performed sequentially – you cannot implement the safeguards/controls unless you know which of them are the most appropriate; you cannot know which safeguards are appropriate before you find out where the potential problems are; if you don't define the rules for the whole process first, it will simply fall apart.

In the next sections, I'll explain each of these steps, using also the guidelines from ISO 27005.

7.3 Writing the risk assessment methodology (clause 6.1.2)

Purpose. As the old saying goes, if you don't know where you're going, you'll probably end up somewhere you didn't hope to arrive. Therefore, you shouldn't start assessing the risks with no methodology in mind, or using some sheet you downloaded somewhere from the Internet (this sheet might be using a methodology that is completely inappropriate for your company); similarly, you shouldn't start using the methodology prescribed by the risk assessment tool you purchased (instead, you should choose the risk assessment tool that fits your methodology, or you may decide you don't need a tool at all, and that you can do it using simple Excel sheets).

What you should do is – you should develop or adapt the methodology to your specific circumstances and to your needs.

Inputs. There are many myths regarding what the risk assessment should look like, but in reality ISO 27001:2013 requirements are not very difficult – here is what clause 6.1.2 requires:

1) Define how to identify the risks that could cause the loss of confidentiality, integrity, and/or availability of your information.

2) Define how to identify the risk owners.

3) Define criteria for assessing consequences and assessing the likelihood of the risk.

4) Define how the risk will be calculated.

5) Define criteria for accepting risks.

So, essentially, you need to define these five elements in your methodology – anything less won't be enough, but more importantly – anything more is not needed, which means: don't complicate things too much.

Also, you need to ensure that the risk assessment results are consistent – that is, you have to define such methodology that will produce comparable results in all the departments of your company.

Options. Of course, there are many options available for the above five elements – here is what you can choose from:

- **Risk identification**. In the 2005 revision of ISO 27001 the methodology for identification was prescribed: you needed to identify assets, threats, and vulnerabilities. The current 2013 revision of ISO 27001 does not require such identification, which means you can identify risks based on your processes, based on your departments, using only threats and not vulnerabilities, or any other methodology you like; however, my personal preference is still the good old assets-threats-vulnerabilities method – for instance, this method will allow you to identify, e.g., all the people who create high risks in your company, and people are very often the weakest link in security.

- **Risk owners**. Basically, you should choose a person who is both interested in resolving a risk, and positioned highly enough in the organization to do something about it.

- **Assessing consequences and likelihood**. You should assess separately the consequences and likelihood for each of your risks; you are completely free to use whichever scales you like – e.g., Low-Medium-High, or 1 to 5, or 1 to 10 – whatever suits you best. Of course, if you want to make it simple, go for Low-Medium-High.

- **Method of risk calculation**. This is usually done through addition of consequences and likelihood (e.g., 2 + 5 = 7) or through multiplication (e.g., 2 x 5 = 10). If you use scales Low-Medium-High, then this is the same as using scale 1-2-3, so you have numbers again for calculation.

- **Criteria for accepting risks**. If your method of risk calculation produces values from 1 to 10, then you can decide that an acceptable level of risk is, e.g., 7 – this would mean that only the risks valued at 8, 9, and 10 need treatment. Alternatively, you can examine each individual risk and decide which should be treated or not based on your insight and experience, using no pre-defined values. In any case, the level of acceptable risk will have to be in line with your business strategy – if you are, e.g., a conservative organization like a bank, then your acceptable level of risk will be lower.

The decision of choosing between these options will depend on the following:

- Size and complexity of your company – the smaller and less complex your organization is, the simpler methodology you should go for.
- Legislation, contractual obligations – if laws and regulations (but also contracts with your clients) require you to use a certain methodology, then you have nothing to think about.
- Existing rules for risk management – if you are a larger corporation or a bank, it is likely you already have some policies for enterprise risk management – your information security risk management must be compliant with them.

Decisions. Since this kind of methodology will have consequences on the number of employees required to perform it, as well as on the precision of the results, it is highly recommended that the final approval of this document is done by top management. Of course, before sending it for approval, you should send it for review to a couple of heads of departments and your project team members.

Documentation. Your methodology document needs to describe the following:

- The risk assessment process, including method of risk identification, how the level of risk is determined, assessment scales, method of risk calculation, how to determine the risk owner, the acceptable level of risk, how the decision on risk treatment is made, which tools to use, etc.
- The risk treatment process, including responsibilities and documentation.
- Laws and regulations, contractual requirements related to your risk management.

- The review period – normally once a year, or more often in the case of some bigger changes. See also section Regular review of the risk assessment and treatment (clause 8.2) 8.9 for details.
- Roles in the whole process – please see sections about performing risk assessment and risk treatment.
- Which documents need to be produced – please see sections about performing risk assessment and risk treatment.
- Who needs to communicate which information to whom, and which reports are needed.
- How to protect the confidentiality of the information produced during the assessment.

Documentation tip: (mandatory) A document called *Risk assessment methodology* or *Risk management methodology*.

7.4 Risk assessment part I: Identifying the risks (clauses 6.1.2 and 8.2)

Purpose. In my experience, the employees (and the organization as a whole) are usually aware of only 25 to 40% of risks – therefore, a thorough and systematic process needs to be carried out to find out everything that could endanger the confidentiality, integrity, and availability of their information.

Options. Since this step in the project could be quite time-consuming and complex, you should decide whether it will be coordinated by the CISO, or by some hired expert (e.g., a consultant) – for the sake of simplicity, I will mention only the CISO in the remainder of this section. In any case, this person has to develop the sheets for

BIBLIOGRAPHY

ISO 9001:2015, Quality management systems – Requirements

ISO 14001:2015, Environmental management systems – Requirements with guidance for use

ISO/IEC 20000-1:2011, Information technology – Service management – Part 1: Service management system requirements

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 27004:2009, Information technology – Security techniques – Information security management – Measurement

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

ISO/IEC 27011:2008, Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC TR 27015:2012, Information technology – Security techniques – Information security management guidelines for financial services

ISO/IEC 27017:2015, Information technology – Security techniques –

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC TR 27019:2013, Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity

ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002

ISO 31000:2009, Risk management – Principles and guidelines

ISO/DIS 45001, Occupational health and safety management systems – Requirements with guidance for use

COBIT 5, ISACA, 2012

ITIL 2011, Axelos, 2011

PCI DSS version 3.2, Payment Card Industry Security Standards Council, 2016

SP800 series, NIST

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

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

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

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

The plain English, step-by-step handbook for information security practitioners

Think and act like a consultant with this comprehensive, practical, and step-by-step guide to ISO 27001 implementation.

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 the ISO 27001 standard.
- ✓ Learn how to start an implementation project.
- ✓ Learn how to write the Information Security Policy and other policies and procedures.
- ✓ Conduct risk assessment and risk treatment.
- ✓ Learn how to structure the required documentation.
- ✓ Learn the certification process and the criteria of certification bodies.
- ✓ All this, and much more…

Written in plain English and leaving the technical jargon to the geeks, *Secure & Simple* 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.