PREPARING FOR ISO CERTIFICATION AUDIT: A PLAIN ENGLISH GUIDE

ISO POCKET BOOK SERIES

03

A Step-by-Step Handbook for ISO Practitioners in Small Businesses

DEJAN KOSUTIC

Preparing for ISO Certification Audit: A Plain English Guide

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

ISO 27001 Risk Management in Plain English

ISO 27001 Annex A Controls in Plain English

Dejan Kosutic

Preparing for ISO Certification Audit: A Plain English Guide

A Step-by-Step Handbook for ISO 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 EPPS Services Ltd
Zavizanska 12, 10000 Zagreb
Croatia
European Union
http://advisera.com/

ISBN: 978-953-8155-00-0

First Edition, 2016

ABOUT THE AUTHOR

Dejan Kosutic is the author of numerous articles, video tutorials, documentation templates, webinars, and courses about ISO 27001, ISO 22301 and other ISO standards. 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. He holds numerous certificates, among them ISO 27001 Lead Auditor and ISO 9001 Lead Auditor.

Click here to see his LinkedIn profile

TABLE OF CONTENTS

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 because they were interested in primarily how to prepare their company for ISO certification.

Therefore, I have created this shorter book, a part of the handbook series, which is focused solely on the issues certification process and how to prepare for it. This book is not focused solely on ISO 27001 – the certification process is the same for any standard, so I have adapted this book in such a way so that it is perfectly acceptable for ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22000, OHSAS 18001, ISO 13485 and IATF 16949.

This book, *Preparing for ISO Certification Audit: A Plain English Guide,* is actually an excerpt from the book *Secure & Simple*, and has been edited with only a few smaller details. So, if you compare the sections from *Secure & Simple* that speak about certification, you'll see the same sections here, with almost the same text – as I mentioned, the text was adapted in a way that it is readable from any ISO standard point of view.

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

You might also be puzzled by the fact that this book is rather short, whereas there are other books on ISO certification 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 preparation for certification in smaller companies – therefore, I have intentionally simplified the steps so that your preparation can be done rather quickly, 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 implementing ISO standard.

So, rest assured: if you are a smaller organization, by using this book you will be able to get yourself ready for the certification audit. And, you will see real benefits of doing the certification for your business.

1
INTRODUCTION

Why would your company go for ISO certification? How is company certification different from personal certification? And, is this book the right choice for you?

This book covers the certification process for all ISO management standards – ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 13485, but also OHSAS 18001 and IATF 16949 (former ISO/TS 16949), so in the book I'll refer to "ISO standard" or simply "standard" to cover any of these standards?

1.1 Why should your company go for the ISO certification?

Before you decide if your company should go for the certification, you have to ask yourself one important question: Do you really need it?

I must tell you there are many organizations who have implemented the standard without going for the certification – one obvious example being banks and other financial institutions. Regulations in most countries are such that they have to implement very strict information security procedures and safeguards, and the majority of them did that using ISO 27001. But, very few of them got certified – they concluded that there was no business reason for them to do so.

And, this is exactly what you need to do – consider carefully if you need the certificate. Here are the potential reasons why you might find the certification useful:

1) **Marketing**. You can use the certificate to get some new clients (because of, e.g., tenders), or to stay in the business (e.g., all your competitors already have the certificate).

2) **Compliance**. In rare cases some regulations will require you to implement particular ISO standard, but you may have cases where you will sign contracts with clients that oblige you to implement e.g. quality management system compliant with ISO 9001. And, instead of having to stand the auditors from each of your clients who want to check whether you have fulfilled the contract, you can have the certification auditor do the job, and then show everyone else the certificate.

3) **Internal pressure**. In some companies, these kinds of projects will never finish unless there is powerful pressure – e.g., a clear deadline. So, if you agree with the certification body on a fixed date for the certification audit, both your management and your employees will have a much stronger sense of urgency for finishing the project.

4) **Objective inputs**. If you want your information security to be implemented in the best possible way, it is good to call in people with high experience and who know how you can benchmark with the best in the industry. Certification auditors will be more than happy to audit someone who is trying really hard and they will provide inputs on what you could improve.

So, if you found at least one of these benefits applicable to your company, then you should probably go for the certification; but, the opposite is also true: if you didn't find yourself in any of these bullets, your company probably doesn’t need the certificate at all.

1.2 Certification vs. registration vs. accreditation

Before moving deeper into the topic of certification, let's clarify some basic things first.

How the company certification works. First of all, ISO standards are published by the International Organization for Standardization – this is an international body founded by governments around the world. Its purpose is to publish standards as a way to deliver knowledge and best practice – as of now, almost 20,000 standards are published in total, and they are recognized in every country.

ISO management standards are only part of these 20,000 standards, which were created primarily as a help for companies to improve their operations in certain areas (e.g., ISO 9001 for quality management, ISO 27001 for information security management, etc.) – this is why most of the talk about these standards is related to companies and their registration, certification, and accreditation.

Certification vs. registration. When you want to say that a company has implemented a standard (e.g., an Environmental Management System according to ISO 14001), has successfully completed the certification audit, and the certification body has issued the certificate, you would normally call this registration or certification.

In North America, the term "registration" is most commonly used, while in the rest of the world it is usually called "certification." So, is there a difference? Technically, yes; but essentially, no.

Certification is when a certification body issues the certificate proving that a company is compliant with a standard; registration is when this certificate is registered with the certification body. So, basically, it comes down to the same thing – a company got a certificate that is formally recognized.

By the way, the International Organization for Standardization recommends usage of the term "certification," so I'll use this term from this point forward in this book.

Certification body vs. registrar. This is the terminology difference that directly arises from the usage of certification/registration terms – in North America people usually use the term registrars, while in the rest of the world they are called certification bodies.

But, again, this is one and the same thing – those are the institutions that perform the certification audits and issue the certificates. Here, also, the ISO recommends using the term "certification body."

Accreditation vs. certification. What is the accreditation, then? In order for certification bodies to be able to perform the certification audits and issue the certificates, they need to get a license – and this license is called "accreditation." So, certification bodies are getting accredited, while companies are getting certified. (The certification body needs to be compliant with the standard ISO 17021 if they want to get accredited for certifying management systems.)

There is usually only one accreditation body for each country (e.g., UKAS for the United Kingdom), while there are several certification bodies operating in each country – ranging from small local certification bodies to large multinational corporations like SGS, BSI, DNV, Bureau Veritas, etc.

The good thing about accreditation bodies is that they usually publish the list of accredited certification bodies in their countries – see here the list of certification bodies in the United

Kingdom, and here the list of certification bodies in United States.

By the way, accreditation bodies also need to be compliant with a standard – this is ISO 17011, a standard which defines the process of accreditation.

Certification for individuals. All the above mentioned was valid for certification of companies – if you want to go for the certification personally, the things are a little different. Many trainings for ISO standards have been developed in order to help you implement a standard in a company, or to audit it. This is also why there are certifications and accreditations related to that training industry.

Regarding the accreditation, there is a similar pattern as described above – if an institution wants to provide training certificates, it should be accredited by an accreditation body, and in this case, such institution needs to be compliant with ISO 17024.

Here are some of the most popular accredited training institutions: PECB, IRCA, Exemplar Global (formerly RABQSA), etc.

Personal certification vs. training certification. In most cases, those accredited training institutions are not delivering the courses directly to students; rather, they have a network of partners – training providers – who deliver the courses under their license and supervision.

This relationship between accredited institutions and training providers usually works in two ways: (a) training providers are using courses developed by accredited institutions, and then the accredited institution issues certificates directly to students, or (b) the training organization develops their own course and an accredited institution certifies such course – in this case, it is common for the training organization to issue the certificate to students, with the approval of the accredited institution.

There are numerous training organizations worldwide – ranging from the certification bodies that also offer the certification of organizations, to small, specialized niche-players and providers of online courses.

It is worth mentioning that certification of courses is mandatory for training providers that provide courses like Lead Auditor, because this is the only way to gain recognition from the certification bodies that will hire auditors with such certificates. However, for other, shorter courses, training providers often choose not to certify their courses because such recognition is not important, and they consider their brand name to be enough of a guarantee of the course quality.

1.3 Who should read this book?

This book is written primarily for beginners in this field and for people with moderate knowledge about ISO certification – I structured this book in such a way that someone with no prior experience or knowledge about ISO standards can quickly understand how the whole certification process works, and what the steps are for its successful completion. However, if you do have experience with the ISO certification, but feel that you still have gaps in your knowledge, you'll also find this book helpful.

So, if you are a production manager, engineer, compliance officer, information security professional, head of an IT department, executive, or a project manager tasked with implementing an ISO standard 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 be ready for the certification audit, so by carefully reading this book you will gain the know-how for your future consulting engagements.

1.4 What this book is not

This book is about the certification of companies; it is not about how to certify persons – although both companies and persons can get an ISO certificate, the purpose and the process for certification are very different.

This book is focused on the steps during the certification process and how to prepare for the certification, but it does not explain how to implement the standard – in section 2.1 you'll see links to articles that explain the steps in the implementation.

This book won't give you finished templates for all your policies, procedures, and plans; however, this book will explain which documents the certification auditor will be looking for.

This book is not a copy of any ISO 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 what kind of compliance the auditor is expecting to see.

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

1.5 Additional resources

Here are some resources that will help you, together with this book, to learn about various ISO standards:

- ISO online courses – free online trainings that will teach you the basics of ISO 9001, ISO 14001 and ISO 27001, including the tips on how to go for the certification
- ISO 27001 free downloads ISO 9001 free downloads and ISO 14001 free downloads – collection of white papers, checklists, diagrams, templates, etc.
- Conformio – cloud-based document management system (DMS) and project management tool focused on ISO standards.
- ISO 27001 Documentation Toolkit – set of all the documentation templates that are required by ISO 27001, with included expert support that will take you step by step towards certification; similar toolkits exist for other ISO standards.
- Official ISO webpage – here you can purchase an official version of any ISO standard.

2
ENSURING YOUR COMPANY PASSES THE CERTIFICATION AUDIT

Frankly, I never met anyone who has enjoyed certification. In most cases, everyone considers it to be a necessary evil and hates the day when the auditor finally arrives. (Or, calls in sick on that day.)

But, it doesn't have to be so – you can get something out of it beside the certificate itself – as I'll explain later, certification auditors are experienced people with a perfect overview of the best practices, and you can learn quite a lot from them. But, you have to approach them in the right way.

2.1 Steps before going for the certification – the final check

Of course, before going for the certification, first you have to implement the standard. Because this book was not intended for describing the implementation, here are the links to articles that will help you with the implementation:

- Checklist of ISO 9001 implementation & certification steps
- List of ISO 14001 implementation steps
- ISO 27001 implementation checklist

- 17 steps for implementing ISO 22301
- 12 steps for ISO 20000 implementation
- 12 Steps for implementation and certification against OHSAS 18001

OK, now you have worked on ISO implementation for months and months, tried to figure out how to make it easier for yourself by reading books and articles, convinced not only your colleagues but also your management that this standard is very useful, but still you have one problem: you are biased.

This project is your child, and you might be inclined to believe that the documents and everything else you prepared are flawless. But, this is never true – you have always left something hanging in the air, you might have even understood some requirement in the wrong way, you might have missed something. Maybe the problem is not in you – there may be someone else in charge of, e.g., measurement, but this person doesn't do the job properly.

All this means you could have problems at the certification. To avoid that, I would recommend you do the final check, which should give you a clear picture of what you need to fix before the certification.

Basically, this is the trick:

- First, check if the **internal audit, management review**, and **corrective actions** are performed.
- Then, go through the list of **mandatory documents** and see if you have all those. These articles will help you:
    - List of mandatory documents required by ISO 9001:2015

  - List of mandatory documents required by ISO 14001:2015
  - List of mandatory documents required by ISO 27001 (2013 revision)
  - Mandatory documents required by ISO 22301
  - List of mandatory documents required by OHSAS 18001

- Check if all the **processes and controls you have planned for have been implemented** – e.g., in ISO 27001 the controls are planned through the document called Risk Treatment Plan.

- Next, read the standard once more and see if your **documentation complies with all the requirements** in the standard.

- Finally, here comes the most difficult part – you need to **walk around your company** (you should also visit some of your partners/suppliers who have a role in your system) and behave as if you were the certification auditor. This basically means you have to ask them one very simple question all over again: Do you perform everything that is written in your documentation? You just need to read what every one of your documents say (policies, procedures, plans, etc.), and check out if the answers you receive are appropriate. To find the truth, you shouldn't rely on their answers only – you also have to dig deeper and search for records that would prove what they are saying.

And, that’s it – once you perform these tasks – for each of your activities, for each of your documents, for each of your major suppliers and partners, you will have a pretty good picture of what works and what needs to be fixed.

When you look more closely, you'll find that these steps resemble very closely the steps that are performed by an internal auditor. So, why do this, you ask? First of all, internal auditors are usually inexperienced persons and you can't expect much of them at their first job; second, it is you who is responsible for the success of the project, and you probably want to make sure everything is ready.

You can also hire someone from outside to perform this final check – this can be done by your consultant if you have one – it is true he cannot perform the internal audit because of the conflict of interest, but nothing is stopping you from hiring him for this final check. And, if the consultant has experience in auditing, all the better.

See also this mini case study in chapter 4: Preparing a telecom company for a certification.

2.2 How to choose a certification body

Price is, of course, the main criterion for choosing your certification body; and, of course, you should ask a couple of certification bodies for their proposals and see what they include in the price.

However, the price is not all – here are some other things you should consider when choosing whom to work with:

- **Reputation**. If you want to use your certificate for marketing purposes, you probably don't want to get the certificate from a body that is known to give them away with no criteria whatsoever. You should choose a certification body with a solid, if not perfect, reputation.

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 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 31000:2009, Risk management – Principles and guidelines

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

http://training.advisera.com/course/iso-27001-internal-auditor-course/ *ISO 27001 Internal Auditor Course*, Advisera.com

INDEX

Preparing for ISO Certification Audit: A Plain English Guide

A Step-by-Step Handbook for ISO Practitioners in Small Businesses

Think and act like an experienced practitioner with this comprehensive, practical, step-by-step guide to certification against ISO 9001, ISO 14001, ISO 27001, or any other ISO management standard.

Author and experienced consultant Dejan Kosutic shares his knowledge and practical wisdom with you in one invaluable book. You will learn:

- ✓ The benefits of ISO certification for your company
- ✓ All the steps in the ISO certification process
- ✓ How to choose the certification body
- ✓ What the certification auditor can and cannot do
- ✓ How to deal with nonconformities
- ✓ How to approach the certification auditor
- ✓ All this, and much more…

Written in easy-to-understand language, *Preparing for ISO Certification Audit: A Plain English Guide* is written for people who are going for the ISO certification for the first time and need clear guidance on how to do it. Whether you're an experienced practitioner or new to the field, it's the only book you'll ever need on the subject.