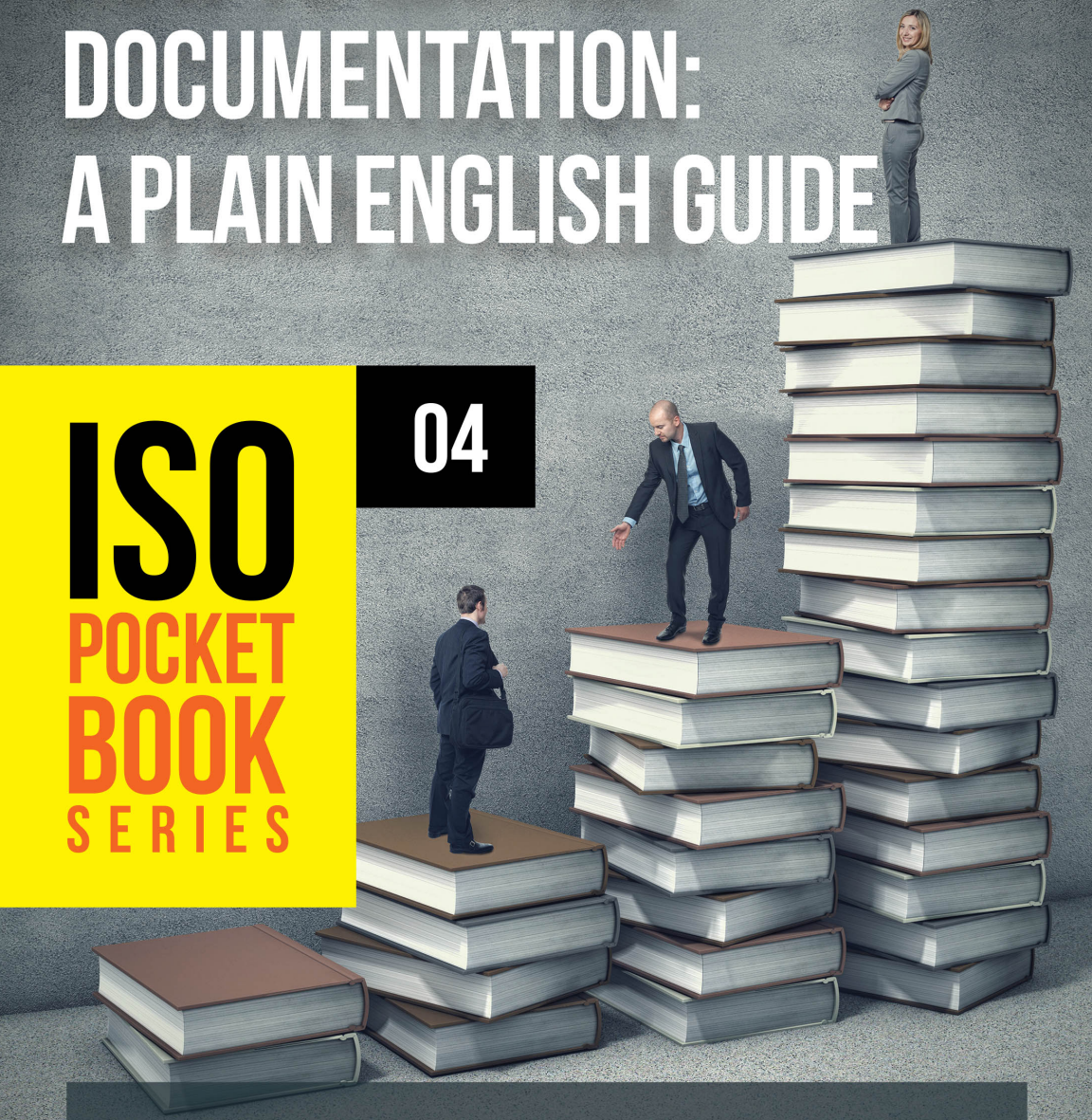
MANAGING ISO DOCUMENTATION: A PLAIN ENGLISH GUIDE



ISO POCKET BOOK SERIES

04

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

DEJAN KOSUTIC

Managing ISO Documentation: A Plain English Guide

Also by Dejan Kosutic:

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

Preparing for ISO Certification Audit: A Plain English Guide

Dejan Kosutic

Managing ISO Documentation: A Plain English Guide

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

Advisera Expert Solutions Ltd
Zagreb, Croatia

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

ISBN: 978-953-8155-01-7

First Edition, 2017

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 last year, very soon I realized many people were reading it because they were interested to learn how to manage the documentation.

Therefore, I have created this shorter book, a part of the handbook series, which is focused solely on the issues of how to handle policies, procedures, plans, and other documents and records. This book is not focused solely on ISO 27001 – the rules for handling documents are 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, *Managing ISO Documentation: 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 documentation, 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 managing documentation, 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 documentation in 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 managing documents in smaller companies – therefore, I have intentionally simplified the description so that you can handle the document in an easy way, 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 manage documents in the most optimal way. And, you will see real benefits of having the appropriate documents that will help you perform your business operations.

1
INTRODUCTION

Why do you need documents and records (or "documented information" as these two are called in ISO standards)? Is this book the right choice for you?

This book covers tips on handling documentation 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 is documentation important for ISO management systems?

Perhaps the most controversial topic about ISO standards is the documentation – there are many different opinions on this, very often completely contrary:

- "We don't need these documents – we're doing just fine without them; this would only be overkill."
- "This standard is all about documentation – we simply need to fill out all the documents, and we'll automatically get the certificate."
- "We need to write policies and procedures for each and every process, activity, and control in our company – the more documents, the clearer the rules will be, and it will be easier for us to comply."

Unfortunately, statements like these can be heard very often. And, unfortunately, none of them reflect the true nature of what ISO standards really require.

The main point of the implementation of any standard is that the employees perform their activities and processes in a better way, and the documentation is here to help you do that, because otherwise, their processes and activities would become unmanageable. Also, the records that are produced will help you measure whether you achieve your objectives and enable you to correct those activities that underperform.

Therefore, you could consider the documentation to be only a tool to achieve better quality (with ISO 9001), security (with ISO 27001), environmental protection (with ISO 14001), etc. – the point is not to write beautiful documents; the point is to improve your business operations.

So, in order to get the biggest benefits from the policies, procedures, plans, and other documents, you need to keep a balance – write only those documents that will really help improve the way you do things, but do not get carried away – the documentation is not an end in itself.

From the perspective of ISO standards, documentation has at least two important roles: to define internal rules that will act as a tool for companies to improve their operations, and to help auditors find out if a company is really complying with the standard. This is why ISO standards place quite a big emphasis on documentation – they specify which documents are mandatory, and in some cases, what the content of particular documents should be.

ISO standards go a step further – they define how various processes and activities (and their documents) fit together, and by doing this they define how to create a management system.

And, as mentioned before – having the documents doesn't mean you have a management system, but without documents your management system wouldn't be possible.

1.2 Who should read this book?

This book is written primarily for beginners in this field and for people with moderate knowledge about ISO documentation – I structured this book in such a way that someone with no prior experience or knowledge about ISO standards can quickly understand how to handle documents and records within the context of ISO standards. However, if you do have experience with the ISO documentation, but feel that you still have gaps in your knowledge, you'll also find this book helpful.

This book provides examples of handling policies, procedures, plans, and other documents 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.

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 writing the documentation – this will be useful when the auditor needs to provide some recommendations in his or her audit report.

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 handle documents, so by carefully reading

this book you will gain the know-how for your future consulting engagements.

So, if you are a production manager, engineer, compliance officer, information security professional, head of an IT department, executive, internal auditor, consultant or a project manager tasked with implementing an ISO standard in a small or mid-sized company, this book is perfect for you.

1.3 How to read this book?

Here are some of the 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 ISO standards, then the standard clause is written in the title of that section.
- Since chapter 3 describes the documentation related to particular clauses of the standard, most of the sections have these elements:
    - **Purpose** – describes briefly why such a clause exists and how it can be used for your management system
    - **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 standard

    - **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 chapters 2 and 3 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 4 you'll see a shorter case study which explains how problem with documentation can be resolved in real situations.
- You'll find lots of useful information in the appendices – glossary, checklists of mandatory documentation for main ISO standards, and structure of documentation for ISO 27001 Annex A.

1.4 What this book is not

This book is focused on how to handle the documentation for ISO standards, but it does not explain how to implement the standard – in section 1.5 you'll see link to free online training that will explain the whole implementation.

This book won't give you finished templates for all your policies, procedures, and plans; however, this book will explain how to prepare your company for writing the documents you really need, and the documents that will be useful rather than an obstacle in your company. But, it doesn't explain how to write each and every document in detail. In Annex A you'll find a list of mandatory documents for each major ISO standard, and also a list of non-mandatory documents that are commonly used.

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 writing documents without actually reading the standard – 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 create documentation
- 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 9001 Documentation Toolkit – set of all the documentation templates that are required by ISO 9001, 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
PREPARING TO WRITE THE DOCUMENTS

One of the most common reasons for failure of ISO projects is that the companies have rushed into such projects without proper preparation. And, part of that preparation is deciding what to do with the documentation.

So, here is what you need to think about in advance:

2.1 Three options for implementing the standard and writing the documentation

At the very beginning of ISO implementation, you're probably overwhelmed with various approaches on how to start and finish such a project successfully. In my opinion, there are three basic options to implement these standards and write all the necessary documents: (1) do it completely using your own employees, (2) use a consultant, or (3) (somewhat in the middle) implement the standard with a Do-It-Yourself approach, while taking advantage of external know-how.

But, not all of these approaches are applicable to everyone – here's an explanation of each of these options, and in which situations they are appropriate.

1) Implementing the standard using your own employees. This is when you decide to implement the standard without any external help, using only the knowledge and the capacity of your own employees. In this option, your employees are doing

all the analysis, performing all the interviews, writing the documentation, etc.

Pros. This is probably the cheapest option because you're not paying for some external service; you're also not allowing anyone from the outside to learn anything about your internal processes or documentation; finally, writing your own documentation increases the commitment of your employees towards the required changes.

Cons. This is probably the slowest option because you're doing everything on your own; if your employees are not experienced or skilled enough, this could prove to be the most expensive option because of the mistakes they could make.

2) Using a consultant. In this option you hire an expert from outside (usually this is a local consultant) who has experience with the implementation of the standard – this person then performs the analysis of your company, does the interviews, writes the documentation, and everything else – basically, he is implementing the whole standard on your behalf.

Pros. This is definitely the quickest way to implement the standard – if you hire a good consultant, he or she will have lots of experience, and will know how to organize the project to finish it quickly; this is also the best way if your employees have no time whatsoever to dedicate to this project. Also, when things need to change, the management might trust someone from outside of the company more.

Cons. Consultants obviously cost money, so this is the most expensive option; further, you are opening access to almost all of your company secrets (e.g., how the company is organized, its main processes and key competitive advantages, who the most important people are, etc.) to an outsider; finally, when someone from outside is writing the documentation, the

employees might feel those policies and procedures are imposed on them, so often they look for ways to bypass them. Further, once the consultant leaves, very often the employees cannot maintain the documentation because they didn't pick up all the necessary knowledge.

3) Implementing the standard with a DIY approach and using external know-how. This option became very popular in the last couple of years, and is basically something in between the first two options. This is where your employees are doing the whole implementation, but they get the know-how, documentation, and support from an external party.

Pros. This option is not as expensive as consultants, and yet you get all the necessary know-how and support; further, you do not open access to your confidential information to anyone from the outside. Also, since your employees are writing the documentation, their commitment to following the new rules will probably be much higher.

Cons. Your employees will still need to learn about the implementation, so this is not the quickest way to implement the standard; also, this option does not resolve the problem if your employees are completely overwhelmed with other projects and have absolutely no time for anything new.

So, which option to choose? You should implement the standard using your own employees if you have employees who already have experience in the implementation, if you have some very confidential data, and if your budget is very low. On the other hand, if you're in a hurry, and are not afraid that some company secrets might be exposed, then you should use a consultant; of course, you'll need a good budget for this option. Finally, choose the Do-It-Yourself implementation option if you want your employees to learn how it's done, if you are not in too much of a hurry, and if your project manager can dedicate a

couple of hours per day for this project; and, of course, if your budget is not too high.

2.2 Sequence of writing the documentation & relationship with PDCA cycle

The good news is: ISO standards have made it easier for you to implement them and to write the documentation by providing you steps in the implementation.

All standards that are compliant with Annex SL (e.g., ISO 9001, ISO 14001, ISO 27001, ISO 22301) are written in a clear and sequential way, so basically your implementation steps should follow almost exactly the same sequence as the standard is written. Or, to be more precise, your steps in the project plan should resemble clauses 4 to 10 of those standards, in the order they are written.

Of course, the output from most of the steps in the implementation will be various documents – you'll need to cover all the mandatory documents, plus all the documents you conclude are necessary for your company. You'll find lists of mandatory documents in the appendices of this book, and in section 3.4 I'll explain how to choose which non-mandatory documents to write.

This sequentiality is a consequence of the standard being written according to the so-called Plan-Do-Check-Act (PDCA) cycle, which says that, in order to have an effective management system, first you need to *Plan* what you intend to do (including setting the objectives), then you have to implement (*Do* phase) what you have planned for, then you have to *Check* whether your implementation has achieved the intended results, and finally, you have to fill the gap (*Act* phase) between what you achieved and what you planned for in the

first place. Since clauses 4 to 10 follow exactly this logic, this is why you should follow it, too.

Please note that when I use the word *implementation* throughout this book I do not necessarily mean only the implementation (Do) phase in the PDCA cycle – by *implementation* I mean any steps that are necessary to apply all requirements of a particular standard, no matter which phase of the PDCA cycle they belong to.

Free tool tip: Conformio is an online tool that covers all the steps in ISO 9001, ISO 14001 and ISO 27001 implementation, and also includes guidelines for each of the implementation steps

2.3 Using tools and templates

When starting to implement a complex framework like ISO standards, you're probably looking for a way to make your job easier. Who wouldn't? After all, reinventing the wheel doesn't sound like a very interesting job.

But, beware when you start looking for such tools – not every tool will help you: you might end up with a truck wheel that doesn't fit the car you're driving.

Types of tools. Let's start first with what types of tools you'll find in the market that are made specifically for ISO standards:

- **Automation tools** – these tools help you semi-automate part of your processes – e.g., managing the project, performing the risk assessment, storing and approving the documentation, managing incidents, assisting in measurement, etc.

- **Tools for writing documentation** – these tools help you develop policies and procedures – usually, they include documentation templates, tutorials for writing documentation, etc.

Pros and cons of automation tools. The basic idea of automation tools is to eliminate time-consuming activities like using spreadsheets for risk assessment in several of your departments – a clever tool will help you merge these results. Automation tools should also help you handle the whole ISO project by suggesting which steps you need to take, who is responsible for what, which documents are to be produced and approved, by whom, etc.

The biggest problem with automation tools is that most of them are made for larger companies: most of these tools are not priced with smaller companies in mind, and even worse – they are made with a multitude of features, so training employees for using such complex tools takes too much time. Therefore, you should definitely consider the ease of use, as well as price before making a decision.

Can you automate everything? One important fact needs to be emphasized here: automation tools cannot help you manage your quality management, environmental protection, information security, etc. For instance, you cannot automate writing your Information Security Policy – to finalize such a document, you need to coordinate your CISO, IT department, and business side of the organization, and only after you reach an agreement can you write this policy. No automation can do that for you.

Yes, you can semi-automate the measurement of success of particular controls, but again, a human needs to interpret those results to understand why the control was performing well or poorly – this part of the process cannot be automated, and neither can the decision on which corrective or preventive

actions need to be taken as a result of gained insight.

Documentation writing tools. You probably won't need tools for writing your policies, procedures, and plans if you already developed your documentation based on a framework that is similar to ISO standard. Also, if you hired a consultant, then it will be his duty to write all the documents.

In other cases, you will find documentation writing tools (i.e., documentation templates) quite useful because they will speed up writing your policies and procedures. The main question here is how to choose the right ones – here are a couple of tips:

- Are they appropriate for your company size? If you are a small company and the templates are made for big companies, they will be overkill for you, and vice versa.
- Which kind of help do you receive for writing documents? Are there any guidelines, tutorials, support, or anything similar that comes with the templates?
- How experienced are the authors? It would be best if the authors have experience in both consulting and auditing, so that the templates are practical for daily operations, but also acceptable for the certification audit.

I must admit I'm quite biased when it comes to tools, since I'm the author of the ISO 27001 Documentation Toolkit and co-author of Conformio, the cloud-based ISO-compliance tool. But, I cannot help it – I really do think that, if you choose the right tool, it can speed up your implementation and make the maintenance of your system easier.

Free tool tip: Conformio is an online tool that provides all the tools for ISO project management – tasks, collaboration, document management, etc.

2.4 Decide on your documentation strategy

Another thing to keep in mind if you want the documentation to work for you, and not the other way around: it is crucial to produce documentation that is optimized for your company's size and complexity.

Number and complexity of documents. Basically, you have to make these decisions before you start your project: (1) do you want a larger or smaller number of documents, and (2) do you want detailed or shorter documents? The more documents you have and the more detailed they are, the more difficult it will be to maintain them and to make your employees observe them. On the other hand, a smaller number of documents that are also quite short might not describe exactly what you need to do.

As a general rule, I recommend my clients not to become too ambitious – if there is no absolute need to create some new document, don't do it; if there is no need to describe some process in great detail, make it shorter. Of course, if there is some requirement from your main client to write a very precise policy, you will probably have to go into detail, but it doesn't mean all of your other documents need to be as detailed.

Mandatory documents. Of course, you will have to write all the mandatory documents – each clause in the standard specifies if the requirement from that clause needs to be documented or not. So, first thing, you need to check whether a document is required by your ISO standard. If the document is mandatory, you have nothing to think about – you must write it if you want to be compliant with this standard. ISO standards state pretty clearly what needs to be documented by simply saying: "The organization shall retain documented information of…," for example, the results of the corrective actions.

(This part of the book is not displayed in the free preview)

BIBLIOGRAPHY

ISO 9001:2015, Quality management systems – Requirements, International Standardization Organization, 2015

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

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

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

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

OHSAS 18001:2007, Occupational health and safety management systems – Requirements, BSI, 2007

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

Kosutic, Dejan, *Secure & Simple*, Zagreb: Advisera Expert Solutions 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

Managing ISO Documentation: A Plain English Guide

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

Think and act like a consultant with this practical guide for managing ISO documentation.

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

- ✓ Sequence of writing documentation
- ✓ How to decide on documentation strategy
- ✓ Whether you should use tools and templates
- ✓ How to control documents and records
- ✓ Which are the mandatory documents
- ✓ How to decide which non-mandatory documents to write
- ✓ How to write documents that will be accepted by your colleagues
- ✓ All this, and much more…

Written in easy-to-understand language, *Managing ISO Documentation: A Plain English Guide* is written for people who are handling ISO documents 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.