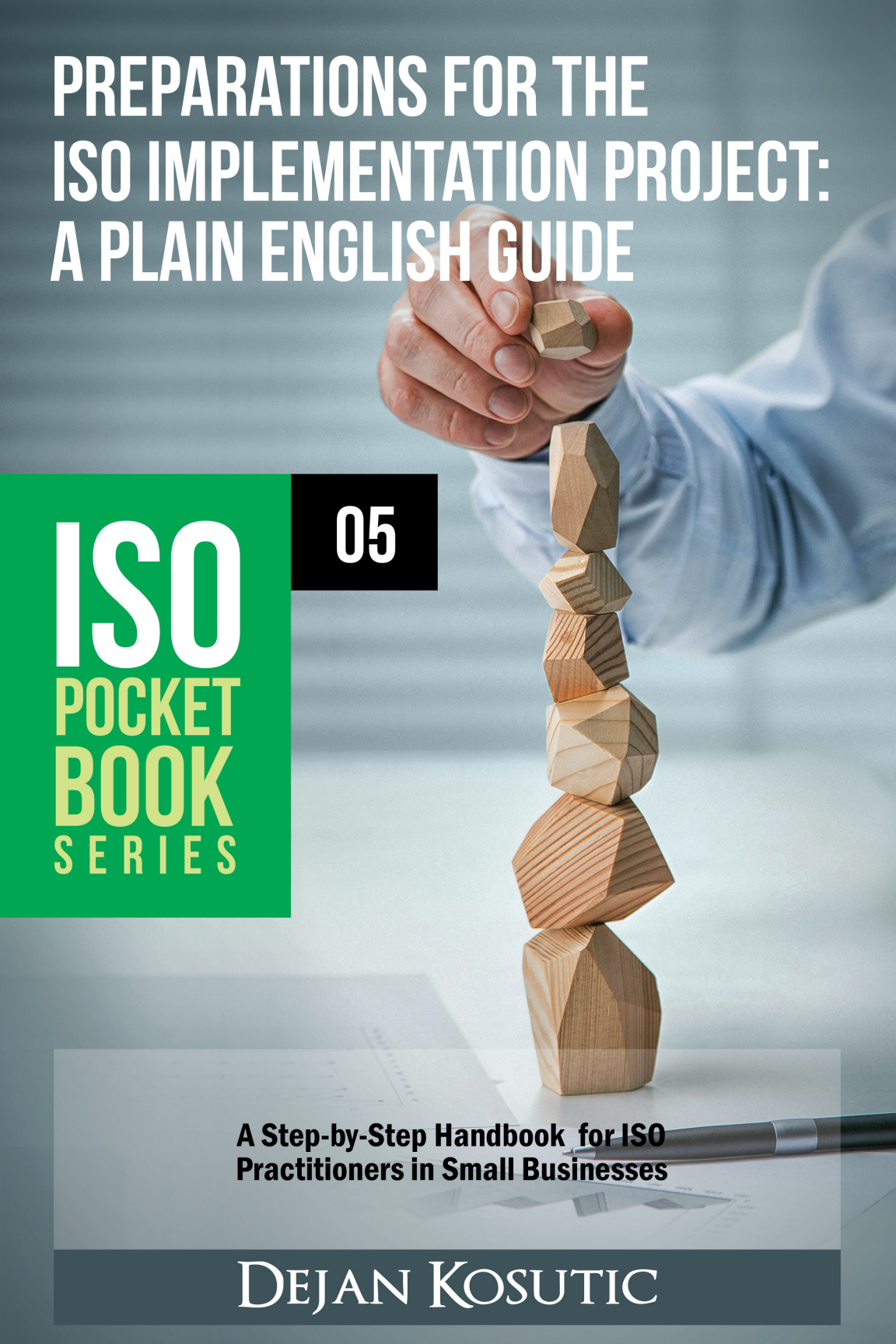
PREPARATIONS FOR THE ISO IMPLEMENTATION PROJECT: A PLAIN ENGLISH GUIDE



ISO POCKET BOOK SERIES

05

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

DEJAN KOSUTIC

Preparations for the ISO Implementation Project: 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

Managing ISO Documentation: A Plain English Guide

Dejan Kosutic

Preparations for the ISO Implementation Project: 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: 978-953-8155-02-4

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

ABOUT THE AUTHOR 5
PREFACE 8

1 INTRODUCTION 10
1.1 FIVE MOST COMMON MYTHS RELATED TO ISO STANDARDS / WHY PREPARATION IS NEEDED 10
1.2 WHO SHOULD READ THIS BOOK? 12
1.3 WHAT THIS BOOK IS NOT 13
1.4 ADDITIONAL RESOURCES 14

2 GETTING THE BUY-IN FROM YOUR MANAGEMENT AND OTHER EMPLOYEES 15
2.1 HOW TO CONVINCE YOUR TOP MANAGEMENT TO IMPLEMENT ISO STANDARD 16
2.2 HOW TO PRESENT THE BENEFITS TO YOUR TOP MANAGEMENT 18
2.3 EXAMPLE OF RETURN ON INVESTMENT (ROI) FOR INFORMATION SECURITY 20
2.4 DEALING WITH LINE MANAGERS AND OTHER EMPLOYEES 22
2.5 SUCCESS FACTORS 24

3 PREPARATIONS FOR THE IMPLEMENTATION PROJECT 25
3.1 STRATEGY FOR ISO IMPLEMENTATION: THREE OPTIONS 25
3.2 HOW TO CHOOSE A CONSULTANT 28
3.3 SHOULD YOU USE GAP ANALYSIS? 30
3.4 SEQUENCE OF IMPLEMENTING ISO STANDARDS & RELATIONSHIP WITH PDCA CYCLE 31
3.5 SETTING UP A PROJECT MANAGEMENT STRUCTURE 32
3.6 WHO SHOULD BE THE PROJECT MANAGER 34
3.7 HOW LONG DOES IT TAKE? 36
3.8 HOW MUCH DOES IT COST? 37
3.9 USING TOOLS AND TEMPLATES 40
3.10 DECIDE ON YOUR DOCUMENTATION STRATEGY 43
3.11 SUCCESS FACTORS 45

4 MINI CASE STUDY: GETTING THE TOP MANAGEMENT COMMITMENT IN A STATE-OWNED COMPANY 47

APPENDIX A – DIAGRAM OF ISO 9001:2015 IMPLEMENTATION 49
APPENDIX B – DIAGRAM OF ISO 14001:2015 IMPLEMENTATION 51
APPENDIX C – DIAGRAM OF ISO 27001:2013 IMPLEMENTATION 53
APPENDIX D – DIAGRAM OF ISO 22301:2012 IMPLEMENTATION 55
APPENDIX E – DIAGRAM OF OHSAS 18001:2007 IMPLEMENTATION 57
APPENDIX F – DIAGRAM OF ISO 13485:2016 IMPLEMENTATION 59
APPENDIX G – TEMPLATE: PROJECT PROPOSAL FOR ISO IMPLEMENTATION 61
APPENDIX H – TEMPLATE: PROJECT PLAN FOR ISO IMPLEMENTATION 66
APPENDIX I – LIST OF QUESTIONS TO ASK YOUR ISO CONSULTANT 72

BIBLIOGRAPHY 76
INDEX 78

PREFACE

When we published my book *Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own* last year, I realized very soon that many people were looking for information on what they need to do to make their ISO implementation successful.

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

This book, *Preparations for ISO Implementation Project: 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 implementation preparation, 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 implementation, 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 similar books 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 preparation for implementation 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 standards.

So, rest assured: if you are a smaller organization, by using this book you will be able to get yourself ready for the implementation of your ISO standard, even though you're doing this for the first time.

1
INTRODUCTION

What are the most costly mistakes you can make with ISO implementation? Why is preparation for ISO project important? And, is this book the right choice for you?

This book covers the preparation for any ISO management standard – 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.

Also, instead of e.g. "QMS" for Quality Management System or "ISMS" for Information Security Management System", I'll simply use the phrase "management system".

1.1 Five most common myths related to ISO standards / Why preparation is needed

There are many misconceptions about ISO standards that very often do not allow the standard to become a serious candidate for consideration, let alone for the actual implementation. In fact, we could call these myths the biggest enemy of ISO standards.

Here's what I hear too often:

"We'll let the administrator handle it."

This is the management's favorite – "We'll give this ISO project to that administrator; he doesn't cost us much anyway." Well, the problem with this approach is that the project is never going

to end –because this administrator doesn't have enough knowledge for this kind of a project, he probably doesn't have enough time, and he certainly doesn't have enough authority.

"We'll implement it in a couple of weeks"

You could implement your ISO standard in two or three weeks, but it won't work – you would only get a bunch of policies and procedures no one cares about. Implementation of a management system means you have to implement changes, and it takes time for changes to be accepted by your employees.

Not to mention that you must implement only those controls or processes that are really needed, and the analysis of what is really needed takes time.

"This standard is all about documentation"

Documentation is an important part of implementation of any ISO standard, but the documentation is not an end in itself. The main point of ISO implementation is that the employees perform their activities in a defined way, and the documentation is here to help you do that. Also, the records that are produced will help you measure whether you achieve the objectives you have set for your management system and enable you to correct those activities that underperform.

So, you could consider the documentation to be a tool to handle your e.g. quality for ISO 9001, environment for ISO 14001, or security for ISO 27001, rather than considering it to be an overkill for your operations.

"The only benefit of the standard is for marketing purposes"

"We are doing this only to get the certificate, aren't we?" This is (unfortunately) the way 80 percent of the companies think. I'm not trying to argue here that ISO standard shouldn't be used in promotional and sales purposes, but you can also achieve

other very important benefits – the main benefits are listed in section 2.1.

"We need a GRC tool to implement ISO standard"

Governance, risk, and compliance tools can indeed be helpful; however, they are by no means required for ISO implementation. You can host all your documentation on your existing server, or on some cloud service like Dropbox, or on your computer; automatic logs should be kept in the systems that created them – you'll find more detailed guidance in section 3.9.

The point I'm making here is this – go through this book to see what is really needed and what is not, and then decide where to invest most of your time and money regarding your ISO project.

The main idea of this book is to help you avoid some costly mistakes – in other words, to prepare yourself for your ISO project instead of hastily rushing into it.

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 implementation – I structured this book in such a way that someone with no prior experience or knowledge about ISO standards can quickly understand how to prepare for an implementation project. However, if you do have experience with the ISO implementation, 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.

This book provides examples of preparing for the implementation of ISO 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 project management structure than the one that is suggested in section 3.5 Setting up a project management structure.

To summarize, this book gives you a systematic picture of the activities you need to do and the decisions you need to make before you start implementing your ISO standard – by using this book you make sure that you don't make some costly mistake at the very beginning.

1.3 What this book is not

This book is focused on the activities and decisions you need to consider before you start your ISO implementation project, but it doesn't explain the actual implementation of any particular ISO standard. (In the next section you'll find references for materials that will help you with the implementation.)

This book won't give you finished templates for all your policies, procedures, and plans; however, in appendices of this book you'll find a couple of templates, for example the Project Plan.

This book is not a copy of any ISO standard – you cannot replace reading the standard by reading this book. So, please don't make the mistake of starting an implementation of a

standard without actually reading it – I think you'll find this book and ISO standard to be the perfect combination for your future work. You can purchase the standard at the ISO official website.

1.4 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 how to implement 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, ISO 14001 free downloads, OHSAS 18001 free downloads and ISO 20000 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 through the implementation; similar toolkits exist for other ISO standards.
- Official ISO webpage – here you can purchase an official version of any ISO standard.

2
GETTING THE BUY-IN FROM YOUR MANAGEMENT AND OTHER EMPLOYEES

There is actually one top reason that most ISO practitioners are emphasizing, that is responsible for the failure of their projects: lack of understanding from top management and, consequently, lack of their continuous support.

However, top management is not the only problem. Very often, ISO practitioners are, if not completely misunderstood, then at least avoided by other employees in a company. By "ISO practitioners," I mean anyone who is in charge of implementing a particular ISO standard.

The solution to this problem? You are probably not going to like this: you have to become a combination of a diplomat and a salesman. You'll have to sell the idea of the standard you're working on to your management, to your employees, and to your partners, and you'll have to use all your power of persuasion to convince them. And no, your job as ISO practitioner is not only about policies and procedures – it is primarily about psychology and convincing people around you.

This chapter will show you how to do this.

2.1 How to convince your top management to implement ISO standard

If you think that your management loves to listen to your great idea about a new policy, or a new technology, you're wrong – they just don't care.

What management wants to hear (and does understand) are profit, market share, client satisfaction, cost cutting, business strategy, and business risks. And you can't blame them – after all, this is what their job is all about.

So, if you can't change them, you have to change yourself. From the very beginning, if you want them to listen to you, you have to start speaking the language they understand – and they will understand only if you present them with the business benefits of implementing your standard.

In my experience, there are four potential benefits you should consider:

1. **Compliance.** There are more and more laws and regulations in almost every country that can be complied with by implementing a particular standard (e.g., personal data protection, protection of classified government information can be resolved by implementing ISO 27001); but, what's even more interesting, is that there is an increasing number of business clients that require their suppliers and partners to implement a particular standard (e.g., a construction company requiring their suppliers to be ISO 9001 certified). The good news is that ISO standards are perfect frameworks for complying with all these requirements, partly because these international standards were a model when those laws and regulations

were developed. This means less effort in the compliance process, and fewer penalties to be paid.

2. **Marketing advantage.** If your company has the ISO certificate and your competitors do not, you could actually gain new clients because you will be able to convince potential clients you have some kind of a capability (e.g., better handling of customer requirements with ISO 9001, higher resilience with ISO 22301, etc.) that your competitors do not. This means increased market share and higher profits.

3. **Lowering the expenses.** ISO standards are usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by e.g., incidents or customer complaints. (You probably do have some kind of security, health & safety, environmental, or other incidents; you also probably have customers complaints – all of these cost you money.) True, it is difficult to calculate how much money you could save if you prevented such incidents/complaints – but it always sounds good if you bring such cases to management's attention. (Later in this chapter I'll explain how to calculate the amount of savings for information security incidents, in section 2.3.)

4. **Optimizing the business processes.** This one is probably the most underrated – if you are a company that has been growing sharply for the last few years, you might experience problems like – who has to decide what, who has to report to whom, who is responsible for what, etc. ISO standards are particularly good in sorting these things out – they will force you to define very precisely roles and responsibilities, and therefore strengthen your internal organization.

I'm not saying all of these four benefits will be applicable to your organization, but chances are you'll find at least two that are really relevant to your organization. And, you have to consult with your colleagues in the company, because you ultimately have to figure out which of these benefits are the most interesting to your top management, and which ones support your company's strategy. The best way to do this would be to brainstorm these benefits with your colleagues from the business side of the organization, and with those in corporate functions.

Of course, you'll also have to find ways you can relate your ISO project with the company business strategy. Here's an example: let's say that your company wants to start offering services in the cloud, which means that the customers' sensitive information need to be protected; if you start implementing ISO 27001, it will not only decrease the likelihood that some data will leak, it will also decrease the unavailability of the service – therefore, such project will support the strategic step your company decided to take.

See also this mini case study in chapter 4: Getting the top management commitment in a state-owned company..

The next step is to figure out how to reach the minds of your management.

2.2 How to present the benefits to your top management

Don't expect your management to grasp all the benefits after a 20-minute meeting, no matter how nice your PowerPoint presentation looks. Unfortunately, it will take time for your management to understand.

Here are a few techniques you can use for presenting your case in a more effective way:

Elevator speech. Chances are you'll achieve much more in informal occasions than in formal meetings – e.g., when you accidentally stumble into your CEO in a cafeteria, in an elevator, or similar. If you are not prepared for such an occasion, you'll probably get confused – therefore, you have to prepare a so-called elevator speech, a 30- to 60-second speech where you vividly present your case. When you rehearse it well, you will sound confident and convincing. For example, my elevator speech (as a consultant trying to sell my services) is: *The investment in ISO 27001 will pay off if you prevent only one medium-sized incident, not to mention large incidents*.

Find an ally. You need to find people who are close to your CEO and who would naturally be interested in what you are doing – for example, your Chief Financial Officer might see implementation of ISO standard as a way to decrease the financial risk to the company, so she may choose to support your effort; the Chief Compliance Officer could see your project as a way to relieve him of part of the workload, while the marketing guys might see this as an additional key selling point. In any case, do your homework and research who would be interested in the benefits mentioned in previous section.

These people will not only give you additional insight into how a particular ISO standard will help the company, they will also make it easier to get to the top management agenda more quickly.

30-20-10 rule. When you do make your PowerPoint presentation, forget about all those fancy statistics you've found, and hundreds of slides you prepared. Instead, go for the 30-20-10 rule: use fonts size 30, maximum 20 minutes, up to 10 slides. And focus on benefits – this is the main message you need to deliver. (See also Appendix G for a project proposal template.)

Careful with words. Remember, your target group is managers who don't understand or don't like your geeky expressions. For example, when presenting information security/ISO 27001:

Instead of:	Use this:
Backup, fire-suppression systems (and other safeguards)	Prevention (*We will prevent...*)
Cost	Investment (*By investing in ..., we will save xyz dollars...*)
Probability	Risk (*We will decrease the risk of...*)
Incident	Damage (*We will decrease the damage by implementing...*)
Disaster	Loss/downtime (*We will lose xyz dollars; our expected downtime will last...*)

Figure 1: Words to avoid and words to use when presenting an ISO project

And, above all, be patient and persistent – behave like a real salesman. After a while, you will surely start to notice some progress – maybe not in the first couple of days or even couple of months, but don't let that discourage you.

2.3 Example of Return on Investment (ROI) for information security

The following example is about information security; however, it can be applied very similarly to environmental incidents, and perhaps even to health & safety incidents.

Very often, you will be asked, "If we invest xyz dollars in your information security, will it pay off? What's the ROI?"

Instead of going into a deep theory of how to calculate the ROI, let me give you a simple example.

Let's say you have a server that, if destroyed, the damage (in hardware, data, and downtime) would be $100,000 – this is also called the Single Lost Expectancy (SLE). Let's say you have a threat of fire, and that such an incident can happen once in 20 years – this means that Annualized Rate of Occurrence (ARO) would be 5%. So, now you have to calculate the value of the risk (or, using this complicated terminology – Annualized Lost Expectancy or ALE), which is calculated by multiplying SLE by ARO.

This means your risk has a value of $5,000 annually.

What does this mean? This means that as long as you invest less than $5,000 in fire-prevention and fire-suppression systems, you will make a profit. So, let's say that you invest $4,000 in those systems per year – this means you make a profit of $1,000 each year. This is the amount of money you have saved your company on average, per year, because with those systems the fire should never happen (i.e., you eliminated the risk).

If you made a profit of $1,000 on a $4,000 investment, this means your ROI is 25% – pretty good, isn't it?

However, the truth is: yes, it is difficult to calculate the damage that would occur; yes, there are no reliable statistics on the frequency of such incidents. But, with effort, you can calculate the damage with relative accuracy and you can make an educated guess on the frequency – and yes, you might miss by 50 or 70 percent, which is still much better than a sheer guess, by which you might miss by 50 or 70 times.

So, the main point here is – unless you give at least some estimate to your management, they won't have the faintest idea about the benefit of your ISO standard in monetary terms. And, when you do come up with dollars and percentages, this is the language they do understand, and that will make them start to listen.

However, inaccuracy in calculations like this is not the only problem – the other problem is that it takes time and a lot of effort. This is why I would recommend using this ROI calculation only if you are proposing some bigger investment (e.g., purchase of some expensive equipment) – in such case, it does make sense to show your management the logic of the numbers.

Free tool tip: This Return on Security Investment calculator gives you the formula to calculate the damage of an incident, and helps you calculate overall ROI.

2.4 Dealing with line managers and other employees

Most employees in your company will be rather skeptical about what you're doing, so you have to sell the idea about ISO implementation to them, too. And, the good news is – getting their buy-in is not very different from getting commitment from top management. Again, you have to find benefits that are relevant to their departments, or to them personally, and present them in a convincing way.

For example, if your head of the Sales department thinks information security is quite unnecessary, ask him the following: "What would happen during the bidding process if the data from your proposal leaked to your competitors?" He would probably answer: "This has never happened so far. I trust my

people." But, then you can provide examples on how this happened, e.g., to other companies in your industry, or perhaps how data already leaked in your company in some other department.

You can take the conversation a step further. Let's say that your Sales department wants to send the proposal to the tender through which they would acquire the biggest customer in the last 3 years. What if such data leak happens in the middle of such process?

Once you have this window of opportunity opened, you have to explain what you can do for him and for his department: you can define exactly who can access which data, where the data is stored, and how it is transmitted – the point is, with relatively little effort, a big incident is prevented.

And, this is how it works with any other standard, with any department, with any individual – from my experience thus far, I have found almost no department in any company that would not benefit from ISO standards.

So, what does this mean to you? Do your homework first. Study your business processes, your main products, what is critical in every department, any important deadlines, etc. Once armed with this knowledge, you will be able to get almost anyone on your side.

Of course, you have to keep repeating these convincing activities in a systematic way – this is normally done through a program of developing awareness, but this is something you'll do during the initial implementation of the standard (and afterwards).

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

BIBLIOGRAPHY

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

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

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

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

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

ISO/DIS 45001, Occupational health and safety management systems – Requirements with guidance for use, International Organization for Standardization, 2015

ITIL 2011, Axelos, 2011

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

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

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

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

accreditation, 12
alarm system, 39
Annex A, 30
Annualized Lost Expectancy ALE), 21
Annualized Rate of Occurrence (ARO), 21
awareness, 23, 40
backup, 39
banks, 28
benefits, 16, 18, 19, 22
budget, 38, 39
business benefits, 24
Business continuity, 76
Business continuity coordinator, 33
Business continuity manager, 33
business continuity plans, 16
business continuity strategy, 39
business continuity tools, 29, 40
business risks, 16
business strategy, 16
CEO, 19, 47, 48
certificate, 17, 28
certification body, 18, 39, 40, 49, 51, 53, 55, 57, 59, 61, 66, 72
Chief Compliance Officer, 19
Chief Financial Officer, 19, 38
client satisfaction, 16
clients, 16, 28, 29, 43
cloud, 12, 14, 18, 42
commitment, 22
communication, 29, 34
company strategy, 18
compliance, 12, 16, 30, 42, 62
consequences, 31
consultant, 19, 28, 29, 39, 80
consulting, 28, 29
cost, 20
cost cutting, 16
costs, 38, 39, 40
courses
course, 28, 35, 39
customers, 28
department head, 38
disaster recovery site, 16
document management system, 14
documentation templates, 39
elevator speech, 19
executives, 40
financial risk, 19
fire-suppression system, 39
fire-suppression systems, 20, 21
Gantt chart, 34
Information security, 76
information security professional, 12
internal audit, 40
International Standardization Organization (ISO), 14
Investment, 20
ISMS, 44
ISO, 76, 77

ISO 22301, 2, 62, 67, 76, 77
ISO 9001, 76
IT administrator, 12, 25
IT company, 28
IT department, 33, 47
ITIL, 76
larger organizations
  large organizations, 13
laws and regulations, 16
Lead Auditor, 28, 73
Lead Auditor Course, 28
Lead Implementer Course, 28
line managers, 24
loss/downtime, 20
market share, 16, 17
measurement, 41, 42
objectives, 31
PDCA cycle, 36
personal data protection, 16
Plan-Do-Check-Act (PDCA)
  cycle, 31, 32
prevention, 20
profit, 16, 17, 21
project management, 32, 34
project manager, 12, 25, 28,
  32, 33, 35, 36, 39, 45, 69,
  70, 71
Project plan, 31, 32
project team, 32, 33, 34
quality manager, 12
recovery plans, 43
resources, 25
risk assessment, 31, 41, 44,
  63, 70, 74
risk treatment, 11, 63
ROI, 21, 22, 24
roles and responsibilities, 17,
  67
safeguards, 20
Sales department, 22, 23
satellite phone, 39
scope, 28
sponsor, 32, 33, 38
Statement of Applicability, 30
strategy, 18, 48
suppliers and partners, 16
surveillance visits, 40
technical controls, 38
threat, 21
top management, 15, 18, 19,
  22, 33
training, 39, 40

Preparations for an ISO Implementation Project: A Plain English Guide

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

Think and act like an experienced implementer with this comprehensive and practical guide that will teach you what preparations you need to make before you start your project for implementing 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:

- ✓ How to convince your top management to implement the standard
- ✓ How to present the business benefits of ISO implementation
- ✓ How to gain the commitment of other employees in your company
- ✓ How to develop your strategy for ISO implementation – learn the 3 options you have
- ✓ How to choose a consultant
- ✓ How to set up a project management structure
- ✓ How long the project will take, and how much it will cost
- ✓ Whether you should use tools and templates
- ✓ All this, and much more…

Written in easy-to-understand language, *Preparations for an ISO Implementation Project: A Plain English Guide* is written for people who are going for an ISO implementation for the first time and need clear guidance on what to do before the project starts. Whether you're an experienced practitioner or new to the field, it's the only book you'll ever need on the subject.