ISO INTERNAL AUDIT: A PLAIN ENGLISH GUIDE

06

ISO POCKET BOOK SERIES

A Step-by-Step Handbook for Internal Auditors in Small Businesses

DEJAN KOSUTIC

ISO Internal 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

Preparing for ISO Certification Audit: A Plain English Guide

Managing ISO Documentation: A Plain English Guide

Preparations for the ISO Implementation Project: A Plain English Guide

Dejan Kosutic

ISO Internal Audit: A Plain English Guide

A Step-by-Step Handbook for Internal Auditors in Small Business

Advisera Expert Solutions Ltd
Zagreb, Croatia

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

ISBN: 978-953-8155-03-1

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**
ACKNOWLEDGMENTS **10**

1 INTRODUCTION **11**
1.1 WHY COMPANIES NEED INTERNAL AUDITS 11
1.2 ISO 19011 – A STANDARD FOCUSED ON AUDITING 12
1.3 WHO SHOULD READ THIS BOOK? 13
1.4 HOW TO READ THIS BOOK 13
1.5 WHAT THIS BOOK IS NOT 14
1.6 ADDITIONAL RESOURCES 15

2 BASIC THINGS ABOUT THE INTERNAL AUDIT **16**
2.1 INTERNAL VS. EXTERNAL AUDIT 16
2.2 THE MAIN PURPOSE OF THE INTERNAL AUDIT 17
2.3 INTERNAL AUDIT REQUIREMENTS IN ISO STANDARDS 18
2.4 SKILLS, COMPETENCES, AND QUALIFICATIONS FOR INTERNAL AUDITOR 19
2.5 AUDIT FINDINGS: NONCONFORMITIES AND OBSERVATIONS 21
2.6 MAJOR AND MINOR NONCONFORMITIES 23
2.7 INTERNAL AUDIT VS. RISK ASSESSMENT 25
2.8 INTERNAL AUDIT VS. GAP ANALYSIS 26

3 ORGANIZING AN INTERNAL AUDIT **28**
3.1 OPTIONS FOR PERFORMING THE INTERNAL AUDIT AND TOP MANAGEMENT ROLE 28
3.2 THREE KEY DOCUMENTS FOR ORGANIZING THE INTERNAL AUDIT 29
3.3 INTERNAL AUDIT PROCEDURE 30
3.4 ANNUAL AUDIT PROGRAM 31
3.5 AUDIT PLAN FOR AN INDIVIDUAL AUDIT 33
3.6 SUCCESS FACTORS 34

4 STEPS IN THE INTERNAL AUDIT PROCESS 35
4.1 Seven steps for performing the internal audit 35
4.2 Performing document review 36
4.3 Creation of the internal audit checklist 38
4.4 Writing the internal audit report 41
4.5 Initiating corrective actions 42
4.6 Corrective action follow-up 43
4.7 Success factors 44

5 PERFORMING THE MAIN PART OF THE AUDIT 45
5.1 Making assumptions: The biggest auditor mistake 45
5.2 Purpose of the opening meeting 46
5.3 Techniques for finding evidence during the on-site audit 47
5.4 Sampling the records 48
5.5 Recording the evidence during the audit 49
5.6 Interviewing techniques for the audit 50
5.7 Closing meeting 52
5.8 Success factors 52

6 BONUS CHAPTER: DEVELOPING AN AUDITING CAREER 54
6.1 How to become a certification auditor 54
6.2 What do the Lead Auditor Course and Lead Implementer Course look like? 55
6.3 Lead Auditor Course vs. Lead Implementer Course – Which one to go for? 56

BIBLIOGRAPHY 58
INDEX 60

PREFACE

When we published our internal auditor online courses on Advisera's eTraining website, we soon realized that there is a huge demand for this topic. And, although the students are quite satisfied with the courses, it became obvious that many were in need of some written materials that would take them through the internal audit.

This is why I have written this shorter book, a part of the handbook series, which is focused solely on how to perform the internal audit. I have written this book in such a way so that it is perfectly acceptable for any management system, including ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22000, OHSAS 18001, ISO 13485, and IATF 16949.

This book, *ISO Internal Audit: A Plain English Guide,* is based mostly on the above-mentioned internal auditor online courses, and has been edited with only a few smaller details. So, if you compare the curriculum from the internal auditor courses, 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 learning materials with almost the same text? Because I wanted to provide a quick, written reference for people who are performing the audit, who might not have the time to join the course each time they want to remind themselves of some detail. I would say that both attending the internal auditor course and reading this book will give you a perfect combination of learning through visual media, and referring to textual media for details.

You might also be puzzled by the fact that this book is rather short, whereas there are other books on ISO audits 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 three answers for this:

First, this book is focused on internal audits only, which are much simpler than certification audits; second, this book is written for internal auditing in smaller companies – therefore, I have intentionally simplified the steps so that your auditing can be done rather quickly, and left out most of the elements that would be needed only for larger companies.

Third, and most important, 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 ISO internal audits.

So, rest assured: if you are an auditor in a smaller organization, by using this book you will be able to perform your first internal audit – it will take you step by step through the whole process, without stress.

ACKNOWLEDGMENTS

Special thanks to Strahinja Stojanovic, who has done a great job of developing the ISO 9001 and ISO 14001 internal auditor online courses that serve as the basis for this book. I'm also grateful to Mark Hammar for his text about gap analysis.

1
INTRODUCTION

Why is the internal audit so important for management systems, and how can it be useful for the company? What will you find in this book? And, is this book the right choice for you?

Note: This book covers the internal audit process for all ISO management standards – ISO 9001, ISO 14001, ISO 27001, ISO 20000, and ISO 13485, but also OHSAS 18001 and IATF 16949 (former ISO/TS 16949) – so when I refer to "ISO standard" or simply "standard," by this I mean any of these standards. Also, when I mention "management system," I mean the system that is compliant with any of these standards – e.g., Quality Management System according to ISO 9001, Information Security Management System according to ISO 27001, etc.

1.1 Why companies need internal audits

From my experience as a certification auditor, the sad truth is that most organizations perform internal audits just to satisfy the certification body.

Such internal audits usually uncover a few minor nonconformities, which do not get deep into the real problems of the company's management system. And this is very unfortunate because this is a waste of time – if companies have invested the time of their internal auditors to perform such jobs, they should gain some benefits out of it.

The point with internal audits is that they should discover problems that would otherwise stay hidden and would therefore harm the business. Let's be realistic – it is human to make

mistakes, so it's impossible to have a system with no errors; it is, however, possible to have a system that improves itself and learns from its mistakes. Internal audits are a crucial part of such a system.

On the positive side, as a certification auditor I did see some organizations performing internal audits in the right way, and for the right reasons. Although their employees did feel a little uncomfortable about the internal auditor checking their activities, very soon they saw the benefits of such an approach – problems became transparent, and were resolved rather soon.

How are these benefits of the internal audit achieved? Here are some tips:

1) The management should view the internal audit as one of the best tools to improve the system, not only as a means to get certified.

2) The internal auditor should be the right person for the job – this means he/she must be qualified, but also motivated and trained to perform this job.

3) The internal audit should be performed in a positive way – the aim should be to improve your system, not to blame the employees for their mistakes.

In this book I'll explain how to achieve all this.

1.2 ISO 19011 – A standard focused on auditing

There is an ISO standard that describes how to perform the audits – it is called ISO 19011. It describes the auditing principles, how to manage the audit program, the required activities during the audit, and the necessary knowledge for auditors.

The principles of ISO 19011 can be used for any type of auditing – a certification audit, an audit of suppliers, and of course, the internal audit.

In this book I included all the main principles of ISO 19011, and scaled them down for the purpose of the internal audit – because the internal audit is not as complex as a certification audit, I have simplified many of the guidelines from ISO 19011 to make them easy to use when performing the internal audit in a small company.

1.3 Who should read this book?

This book is written primarily for beginners in internal auditing and for people with moderate knowledge about internal audits – I structured this book in such a way that someone with no prior experience or knowledge about internal audits can quickly understand how the whole audit process works, and what the steps are for its successful completion.

On the other hand, if you do have experience with internal audits, but you feel that you still have gaps in your knowledge, you'll also find this book helpful.

1.4 How to read this book

This book is written as a step-by-step guide for auditing, and Chapters 2 to 5 should be read in the exact order they are written, because this sequence represents the best way of planning and performing an internal audit.

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

- Some sections contain tips for free tools and for documents that are to be used during the internal audit.
- At the ends of the most important chapters, you'll see a section called "Success factors," which will emphasize what you need to focus on.
- At the end of this book you'll see a chapter that will help you decide whether you want to pursue your career in becoming a certification auditor.

1.5 What this book is not

This book is about the internal audit process; it is not about how to certify your company or how to implement the standard – the implementation process is quite lengthy and involves a lot of steps that are outside the scope of this book.

This book won't give you finished templates for internal audit policies, procedures, and plans; however, this book will explain which documents you will need to perform an internal audit, and how to structure those documents.

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 ISO clauses about the internal audit, and describe best practices when performing the internal audit.

Because this book is focused on internal auditing, it does not explain other elements of ISO standards like document management, risk management, operations, measurement, etc.

1.6 Additional resources

Here are some resources that will help you, together with this book, to learn about internal auditing:

- ISO online courses – free online trainings for ISO 9001, ISO 14001, and ISO 27001 internal auditors.
- ISO 27001 free downloads, ISO 9001 free downloads, and ISO 14001 free downloads – a collection of white papers, checklists, diagrams, templates, etc.
- Conformio – a cloud-based document management system (DMS) and project management tool focused on ISO standards that can be used for auditing purposes.
- ISO 9001 Internal Audit Toolkit – a set of all the documentation templates that are required for performing the internal audit; similar toolkits exist for other ISO standards.
- Official ISO webpage – here you can purchase an official version of any ISO standard.

2
BASIC THINGS ABOUT THE INTERNAL AUDIT

In this chapter I'll give you an overview of the internal audit in the ISO world – its main purpose, how it is different from external (certification) auditing, the exact requirements of ISO standards, how you should select an internal auditor, the main outputs of the internal audit job, etc.

2.1 Internal vs. external audit

As mentioned earlier, ISO 19011 is a standard that describes how to perform audits – this standard defines an internal audit as "conducted by, or on behalf of, the organization itself for management review and other internal purposes." This basically means that the internal audit is performed by your own employees, or you can hire someone from outside of your company to perform the audit on behalf of your company.

On the other hand, the external audit is done by a third party on their own behalf – in the ISO world, the certification audit is the most common type of external audit done by the certification body.

You can also understand the difference between internal and external audit in the following way: the results of the internal audit will be used only internally in your company, while the results of the external audit will be used externally as well – for example, if you pass the certification audit you will get a certificate, which will be used publically. On the other hand, the

focus of the internal audit will be on how to improve your management system, as I'll explain in the next section.

2.2 The main purpose of the internal audit

Unfortunately, the purpose of the internal audit is very often misunderstood – it is usually perceived as a bureaucratic activity with no real benefit. However, the main purpose of the internal audit is to help improve the way your system is managed in your company – this improvement is possible because the auditor is in the perfect position to see what's going wrong, and by having this deeper insight, he or she can help resolve these problems.

The benefits of the internal audit are manifold. In addition to the improvement of your management system, the internal audit is the key source of information for the management review. Also, a very important aspect is that through internal audit the employee awareness is raised for, e.g., quality issues in your QMS (Quality Management System) or information security issues in your ISMS (Information Security Management System), as well as their participation in improving the management system.

To be able to achieve all this, the internal auditor must approach this whole job in a positive way – this means she cannot insult people if she sees that they have made a mistake; rather, she should explain the mistake in a very diplomatic way, and help them improve the way they do things.

I'll explain how the auditor can achieve this in the following chapters.

2.3 Internal audit requirements in ISO standards

The latest revisions of ISO 9001, ISO 14001, ISO 27001, ISO 22301, ISO 13485, and IATF 16949 are aligned and their requirements for the internal audit are basically the same:

- Internal audits must be performed at planned intervals – typically, once a year every department within the scope of your management system must be audited.
- The auditor must check out whether your activities are compliant with the standard, as well as with your own policies, procedures, and other documentation.
- The auditor must also check if the system is properly maintained, meaning that all the documentation is up to date, that all the KPIs are monitored, that corrective actions are performed, etc.
- The company must write the audit program – I'll explain later what this document stands for.
- The company must define the scope of the audit – that is, which departments, processes, or activities will be covered. Typically, you have to cover the whole scope of your management system within one year.
- You also have to define the audit criteria – that is, against which requirements will your management system be audited. Typically, the audit will be made against the standard, against your own documentation, and against some third-party requirements for your management system (for example, this could be some legislation in your country, working instructions given by your partners, etc.).

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

BIBLIOGRAPHY

IATF 16949:2016, Quality management system requirements for automotive production and relevant service parts organizations, International Automotive Task Force, 2016

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

ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes, International Organization for Standardization, 2016

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

ISO 19011:2011, Guidelines for auditing management systems, International Organization for Standardization, 2011

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

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

accreditation, 12
activities, 29
audit conclusions, 41
audit criteria, 18, 21, 32, 41
audit findings, 21, 41
audit plan, 28, 33, 34, 35, 36, 37, 46
audit program, 29, 30, 31, 32, 34
banks, 28
business continuity, 58
certification body, 54, 55
closing meeting, 52
cloud, 15
consultant, 29, 61
corrective actions, 18, 21, 36, 37, 38, 42, 43, 45
courses
  course, 55, 56
document management
  system, 15
document review, 35, 36, 37, 38, 40, 45
IATF 16949, 8, 11, 18
Information security, 58
interested parties, 40
internal audit, 28, 29, 40
internal audit checklist, 35, 38, 40, 61
internal audit procedure, 30, 31
Internal audit report, 37, 41, 42
internal auditor, 28, 29
Internal auditor course, 21
ISMS, 55
ISO, 58
ISO 13485, 8, 11, 18
ISO 14001, 8, 11, 15, 18, 32, 58, 61
ISO 19011, 12, 16, 58
ISO 20000, 8, 11
ISO 22301, 2, 58
ISO 27001, 2, 8, 11, 15, 18, 22, 29, 32, 39, 40, 54, 56, 58, 59, 61
ISO 9001, 8, 11, 15, 18, 41, 58, 61
larger organizations
  large organizations, 28
Lead Auditor, 54, 55
legislation, 29
main audit, 35, 36, 37, 38, 39, 40, 46
Major nonconformities, 24
minor nonconformities, 23, 24, 25
nonconformity, 21, 22, 23, 24, 25, 41, 42, 43, 45, 48, 51
observations, 22, 42
OHSAS 18001, 8, 11
opening meeting, 46
team leader, 32, 34
top management, 29
work documents, 35, 40

ISO Internal Audit: A Plain English Guide

A Step-by-Step Handbook for Internal Auditors in Small Businesses

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

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

- ✓ Internal audit requirements in ISO standards
- ✓ Skills, competences, and qualifications of internal auditors
- ✓ Which documentation is necessary for performing the internal audit
- ✓ 7 steps for performing the internal audit
- ✓ How to develop the internal audit checklist
- ✓ How to collect the evidence and perform interviews
- ✓ How to write nonconformities and internal audit reports
- ✓ All this, and much more…

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