


# ISO INTERNAL AUDIT: A PLAIN ENGLISH GUIDE

The background of the cover features a photograph of a person in a dark pinstripe suit and white shirt. They are holding a document with various charts, including a pie chart and several bar charts. The document is held over a laptop, with the keyboard visible in the lower right. The overall scene suggests a professional business environment.

**ISO**  
**POCKET**  
**BOOK**  
**SERIES**

**06**

**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

Copyright ©2017 by Dejan Kosutic

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the author, except for the inclusion of brief quotations in a review.

**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 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](#)

[PREFACE](#)

[ACKNOWLEDGMENTS](#)

## [1 INTRODUCTION](#)

[1.1 WHY COMPANIES NEED INTERNAL AUDITS](#)

[1.2 ISO 19011 – A STANDARD FOCUSED ON AUDITING](#)

[1.3 WHO SHOULD READ THIS BOOK?](#)

[1.4 HOW TO READ THIS BOOK](#)

[1.5 WHAT THIS BOOK IS NOT](#)

[1.6 ADDITIONAL RESOURCES](#)

## [2 BASIC THINGS ABOUT THE INTERNAL AUDIT](#)

[2.1 INTERNAL VS. EXTERNAL AUDIT](#)

[2.2 THE MAIN PURPOSE OF THE INTERNAL AUDIT](#)

[2.3 INTERNAL AUDIT REQUIREMENTS IN ISO STANDARDS](#)

[2.4 SKILLS, COMPETENCES, AND QUALIFICATIONS FOR INTERNAL AUDITOR](#)

[2.5 AUDIT FINDINGS: NONCONFORMITIES AND OBSERVATIONS](#)

[2.6 MAJOR AND MINOR NONCONFORMITIES](#)

[2.7 INTERNAL AUDIT VS. RISK ASSESSMENT](#)

[2.8 INTERNAL AUDIT VS. GAP ANALYSIS](#)

## [3 ORGANIZING AN INTERNAL AUDIT](#)

[3.1 OPTIONS FOR PERFORMING THE INTERNAL AUDIT AND TOP MANAGEMENT ROLE](#)

[3.2 THREE KEY DOCUMENTS FOR ORGANIZING THE INTERNAL AUDIT](#)

[3.3 INTERNAL AUDIT PROCEDURE](#)

[3.4 ANNUAL AUDIT PROGRAM](#)

[3.5 AUDIT PLAN FOR AN INDIVIDUAL AUDIT](#)

[3.6 SUCCESS FACTORS](#)

## [4 STEPS IN THE INTERNAL AUDIT PROCESS](#)

[4.1 SEVEN STEPS FOR PERFORMING THE INTERNAL AUDIT](#)

[4.2 PERFORMING DOCUMENT REVIEW](#)

[4.3 CREATION OF THE INTERNAL AUDIT CHECKLIST](#)

[4.4 WRITING THE INTERNAL AUDIT REPORT](#)

[4.5 INITIATING CORRECTIVE ACTIONS](#)

[4.6 CORRECTIVE ACTION FOLLOW-UP](#)

[4.7 SUCCESS FACTORS](#)

## [5 PERFORMING THE MAIN PART OF THE AUDIT](#)

[5.1 MAKING ASSUMPTIONS: THE BIGGEST AUDITOR MISTAKE](#)

[5.2 PURPOSE OF THE OPENING MEETING](#)

[5.3 TECHNIQUES FOR FINDING EVIDENCE DURING THE ON-SITE AUDIT](#)

[5.4 SAMPLING THE RECORDS](#)

[5.5 RECORDING THE EVIDENCE DURING THE AUDIT](#)

[5.6 INTERVIEWING TECHNIQUES FOR THE AUDIT](#)

[5.7 CLOSING MEETING](#)

[5.8 SUCCESS FACTORS](#)

## [6 BONUS CHAPTER: DEVELOPING AN AUDITING CAREER](#)

[6.1 HOW TO BECOME A CERTIFICATION AUDITOR](#)

[6.2 WHAT DO THE LEAD AUDITOR COURSE AND LEAD IMPLEMENTER COURSE LOOK LIKE?](#)

[6.3 LEAD AUDITOR COURSE VS. LEAD IMPLEMENTER COURSE – WHICH ONE TO GO FOR?](#)

## [BIBLIOGRAPHY](#)



# 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.).
- The internal auditors may not have any conflicts of interest – this means that if an auditor is working in department A, he can audit all the other departments; however, some other auditor should audit this department A.
- The auditor must write the audit report and present it to the management – more details about this report will be discussed further on in the book.

## **2.4 Skills, competences, and qualifications for internal auditor**

---

There are many skills, competencies, and qualifications that can help a person become an internal auditor, and it is a commonly held belief in the business community that a combination of all three can help an auditor become effective. So, besides avoiding conflicts of interest, here are the other desirable attributes:

**Formal training.** Whether provided externally or internally, formal auditor training can assist in giving your auditor a foundation for becoming an effective internal auditor. There are many training options available, but it pays to research your training provider to ensure the quality of training offered is of an acceptable standard in your industry.

**Education.** Though not considered mandatory for a position like this, people with qualifications in certain disciplines may prove more effective auditors than others – think accountants, financial planners, or warehouse managers, for example – the disciplines and education gained to attain these jobs may be more conducive to auditing skills than others.

**Competencies.** Employees with certain skills, again, may be more effective auditors than others. People who perform stock counts or design complex products may have a superior eye for detail compared to individuals who work in more creative fields, for example. It may pay to take this particular personality trait into account when considering a candidate for internal audit training.

**Personality.** As indicated above, certain people may have better personalities than others for this task. In addition to a strong attention to detail, it pays to have an internal auditor who is curious and questions things. The auditor also needs to be personable and an effective communicator, too, as this function will undoubtedly require a great deal of contact with other employees and other stakeholders.

**Related knowledge.** Obviously, having knowledge of the particular ISO standard is vital to the internal audit function in terms of ensuring your management system meets all your legislative and standard compliances. Also, the internal auditor will be much more effective at this element if he/she has knowledge of the internal process, and all related inputs and outputs.

**Experience.** It stands to reason that experience with the internal audit function, company processes in general, and similar elements in previous roles can help the auditor be effective. An experienced employee will tend to have an edge over a new employee when analyzing the critical issues for examination at internal audit.

**Insight into your industry.** This is particularly important if you're hiring someone from outside of your company – for instance, if you are a construction company, and this person has no idea how the construction industry operates, then you won't have much use for this auditor.

Finally, your company must have the records to prove all this – for instance, if your candidate holds a certificate from an internal auditor course, it will prove that he knows the standard and that he has the skills to perform the internal audit; to prove his experience in the industry, the CV of an auditor will be enough, etc.



***Free tool tip:*** Here you'll find free online trainings for internal auditors for various ISO standards: [Advisera eTraining](#).

## 2.5 Audit findings: Nonconformities and observations

---

Essentially, the internal audit can produce two outcomes: nonconformities and observations. These results are also called the “audit findings.” These outcomes must be documented in the internal audit report, as I'll explain later on.

**Nonconformities.** The definition of a nonconformity is actually very simple: a nonconformity results when a certain requirement is not complied with. Nonconformities are raised when the auditor has found evidence that some aspects of the operations of the company are not aligned with the written procedures (policies, instructions etc.) or with the requirements from the standard. In the context of ISO standards, the requirements (also

called *audit criteria*) might be the following:

- The ISO standard itself – a company must comply with all the requirements written in the standard. So, for example, if corrective actions or management reviews are not documented, this is a nonconformity.
- Legislation – of course, a company must comply with all the local laws and regulations that are relevant for their management system. For example, with the information security/ISO 27001 implementation, the applicable legislation is usually related to personal data protection, cryptography, intellectual property rights, e-services, classified information, etc.
- The organization's own policies and procedures – this means a company must also comply with its own internal rules. For example, setting the objectives must be performed in the way that is described by a top-level policy or some other document.
- Requirements of interested parties – for example, an interested party could be a partner or a client, and you have to comply with their demands as well.

So, the point is, if a company is not complying with any of these four types of requirements, then an auditor must raise a nonconformity.

But, there is also another important point here: if there is no requirement, then a nonconformity cannot be raised. For example, the auditor may believe that management review should be conducted twice a year instead of once; however, if there is no such requirement, the auditor cannot raise a nonconformity.

**Observations.** On the other hand, observations can be raised in different situations, and they can be either positive or negative. A negative observation would be raised when the auditor identifies some kind of deviation from the normal operations, or some practice that could become a nonconformity in the future. An observation might also be raised when there is some isolated case of not following the company policies and

procedures, but which does not influence the effectiveness of the management system – for example, the management review procedure states that the management review meeting is performed at the end of the year, but this year the management review was performed at the beginning of January because the top management was not available earlier.

Also, positive observations can be raised when the auditor identifies an opportunity for improvement; i.e., the auditor thinks that some activities could be done in a better way, although there is no requirement for something like that – for example, the auditor may conclude that internal trainings could be done online instead of holding classroom-type courses, because this would be quicker and more cost-effective.

Additionally, observations can also be used in a more positive way – such as the auditor taking note of a good implementation of some part of the management system, so that this positive example can be used as a role model for other parts of the organization. For example, some departments might demonstrate a much higher level of awareness for environmental protection, so their experience in raising awareness can be used throughout whole organization.

## 2.6 Major and minor nonconformities

---

Classification of nonconformities into “major” and “minor” is mandatory for certification audits; however, it does not have to be used for internal audits. In certification audits, a major nonconformity means that a big problem exists, and that the certificate cannot be issued. However, if you want to, you can classify the nonconformities you have raised during the internal audit as major if you want to emphasize certain problems – that way, those nonconformities will be resolved more quickly.

Now, let’s see how the certification bodies distinguish between major and minor nonconformities.

So, what is considered to be a **major nonconformity**? This would be a nonconformity that has any of these characteristics:

- If a company completely failed to fulfill a certain requirement – e.g., it didn't perform management review at all, although this was required by the standard.
- If your process has completely fallen apart – e.g., your procedure required you to perform backup once a day, whereas the backup was performed only a couple of times per month, randomly.
- If you have several minor nonconformities that are related to the same process or to the same element of your management system – e.g., you have several minor nonconformities related to your Human Resources department: some of the training records are missing, not all employees are trained as they should be, some of the employment records are missing, etc. – this becomes a major nonconformity because there is obviously something very wrong with this department.
- If a certification mark is misused – e.g., you claim to your customers that your product is ISO certified (certification of ISO management standards covers only the processes and management systems, not the products themselves).
- If a minor nonconformity raised during the previous audit was not resolved before the deadline – this minor nonconformity automatically becomes a major one.

The definition of a **minor nonconformity** is easy: this is any nonconformity that is not major; for example, a minor nonconformity could be that the required daily backup was performed every day except one day of one particular month.

So, to conclude, if you don't think that a nonconformity should be classified as major, then it is a minor nonconformity.

Again, using this classification of major and minor nonconformities is not mandatory for internal audits, but you can use it if you feel it will help your company resolve the problems in a better way.



## 2.7 Internal audit vs. risk assessment

---

Quite often, I see people searching for checklists for performing the internal audit; however, it's clear that they are interested in finding out about what potential problems could happen to their operations, their systems, etc.

The problem is – these kinds of things are not part of an internal audit; this is part of the risk assessment.

The purpose of risk assessment is to find out which incidents can jeopardize your management system – consequently, risk assessment needs to be done at the beginning of the ISO project, while the internal audit is done only after the implementation has been completed.

**How is the internal audit different?** The internal audit, on the other hand, is nothing more than listing all the internal rules and ISO requirements, and then finding out if those rules and requirements are complied with.

When performing an internal audit, you need to check if each and every rule and requirement was complied with, in the whole scope of your management system.

**The main differences between the two.** So, I would say that one of the main differences is in the mindset: risk assessment is thinking about the (potential) things that could happen in the future, while the internal audit is dealing with how things were done in the past.

The second major difference is that the internal audit focuses on compliance with various rules and requirements, while risk assessment is nothing more than analysis that provides a basis for building up certain rules.

The third difference is that the risk assessment is done before you start applying the processes and controls, while the internal audit is performed once these are already implemented.

## 2.8 Internal audit vs. gap analysis

---

If you are thinking of implementing a management system according to any of the ISO standards, you will likely have heard the term “gap analysis.” This term is often used interchangeably with internal audit, and although they use similar skills when gathering data, the focus for each is very different. Here is a bit more about these differences.

**Gap analysis.** Even if there is no formal management system established, every company has some, e.g., quality management processes in place to interact with customers, take orders, plan and create products or services, and deliver these to customers in order to be paid. If these processes were not in place, a company would not last long. It is this set of processes that is usually being assessed during a gap analysis.

A gap analysis is mainly done at the beginning of the project to assess what is currently in place against the set of requirements that are going to be used for the implementation. In the case of ISO 9001, you would take each requirement, compare it to what is currently being done, and assess where there is more required for the process currently in place.

**Internal audit.** By comparison, an internal audit is used to assess a process against the procedure that it is supposed to follow, as well as checking that the process complies with the requirements of the standard. The audit will gather audit evidence and compare it to the criteria for the process to see if the criteria are fulfilled. In other words, if your process says you will do something, do you have the evidence to show that you do? This evidence could come in the form of records, statements of fact, or by observing personnel doing the job. This internal audit assessment is done on-site, whereas the gap analysis is commonly done much more superficially through a questionnaire, document review, or similar tool.

**Different, but similar.** While both the gap analysis and internal audit involve comparing a process with a set of requirements, the focus of each is very different. The gap analysis is focused on what is missing in the processes compared to a set of requirements (typically before an implementation takes place), while an internal audit is centered on verifying that the process conforms to the requirements and is effective after the process is already in place per the ISO requirements. A gap analysis deals with identifying missing components of a process, but an internal audit

concerns maintaining an effective process once it is in place. Both are very useful and have their place, but it is important to use each when it is appropriate.

# 3

## ORGANIZING AN INTERNAL AUDIT

This chapter will explain what options you have for the internal audit and how to prepare before you begin, including creating the internal audit program and internal audit plan.

Organizing the internal audit includes defining the internal audit process, as well as creating the procedure together with all necessary documents. This stage is very important because you will define all activities of the internal audit, the content of the records used during the audit, and the necessary competence of the auditors.

### 3.1 Options for performing the internal audit and top management role

---

There are a few ways to perform an internal audit:

- a) **Employ a full-time internal auditor.** This is suitable only for larger organizations who would have enough work for such a person (some types of organizations – e.g., banks – are obliged by law to have such functions).
- b) **Employ part-time internal auditors.** This is the most common situation – the organizations use their own employees to perform internal audits, who do so when required (e.g., a couple of times a year) alongside their regular work. One important thing to pay attention to: in order to avoid any conflict of interest (auditors cannot audit their own work), there should be at least two internal auditors so that one could audit the regular job of the other.

**c) Employ an internal auditor from outside of the organization.**

Although this is not a person employed in the organization, it is still considered an internal audit because the audit is performed by the organization itself, according to its own rules. Usually, this is done by a person who is knowledgeable in this field (independent consultant or similar).

The selection of the above options depends, of course, on whether you have already implemented any ISO standard, and which profile of internal auditor you have. You should also study the legislation, because some industries (e.g., financial) have special rules regarding internal audits.

Your top management must get involved here – from selecting the most appropriate option and appointing the internal auditor, to approving the key documents mentioned in the next section. These activities should not be delegated to lower levels in the hierarchy, because this could bring the internal auditor into a conflict of interest, and besides, some important information might not find its way to the top.

And, most important of all, top management should make a conscious decision that they will accept and support the internal audit as something that is useful for the business.

## **3.2 Three key documents for organizing the internal audit**

---

Let's see what you need in order to organize and plan your internal audit. You'll basically do this through three documents: internal audit procedure, audit program, and audit plan. Out of these three, ISO standards require you to document only the audit program, but it is common to write all three because they are all quite helpful for performing the internal audit.

With the internal audit procedure, your company will define the responsibilities for internal audit, the audit process, the main rules, etc. With the audit program you'll determine when you will perform each audit – normally, this program is written for a period of one year. Finally, with the

audit plan you'll determine the details of each audit.

Now let's see how to write each of these three documents.

### 3.3 Internal audit procedure

---

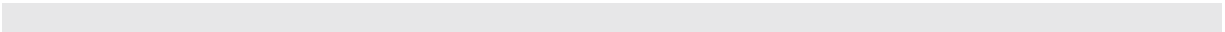
ISO standards do not specify what you should write in the internal audit procedure; however, it would be useful to include the following:

- The purpose of the internal audits, and what your company should achieve when performing those audits.
- Who is in charge of the internal audit planning, and in which cases an internal audit must be performed.
- The criteria for selecting the internal auditors, and who is in charge of appointing the auditors.
- The mandatory steps and mandatory documents when performing the audit.
- And, finally, how to report the internal audit results, and who is in charge of the follow-up based on these results.

Of course, because the requirements of ISO management standards are the same, you can write one procedure that will be used by different management systems; further, if you have skilled auditors in several standards, this means you can perform the audit of more management systems at the same time.

Later on I'll explain the steps of performing an internal audit and how to report the internal audit results, so then you'll be able to develop this procedure fully.

As mentioned before, ISO standards do not require this procedure to be actually written down – you can agree verbally with your colleagues about all these rules, but it will be easier if they are documented.





**Documentation tip:** (non-mandatory) A procedure that describes the internal audit process, usually called the *internal audit procedure*.

## 3.4 Annual audit program

---

As opposed to the internal audit procedure, ISO standards do require you to write the audit program, and you should include the following elements in this document:

- For **which period** you are planning the audits – typically one year, but in some cases this could be three years.
- When the **individual audits** will be performed within this period – for a smaller company, only one audit that covers the whole scope of your management system will be enough; for a mid-sized company that has 10 main departments, you might want to plan 10 audits within this one-year period.
- The **scope** of each audit – define precisely what each audit will cover. For example, the scope can be defined by taking into consideration the location of the audit – so the scope might only include two out of the company's 10 locations; the scope can include only a few processes – for example, the scope might only include the sales process and manufacturing process (have in mind that the sales *process* is not same as the sales *department*, although the sales department is the main actor in the process, while other functions and departments are also involved in the sales process, such as management, technical experts, etc.)
- The **audit criteria/objectives** – as mentioned in the previous chapter, your audit criteria might be the ISO standard, your own documentation, and some third-party requirements for your management system. These audit criteria are very often

referred to as “audit objectives” – e.g., *the internal audit objective is to check the system’s compliance with ISO 14001.*

- Which **methods** will be used for auditing – typically, these will be reviewing the documentation, interviewing the employees, and observation of the activities – I’ll explain these techniques later on.
- And, finally, **who** will be performing the audit – will this be done by one person only, or by several persons? If more than one, who will be their team leader?

When creating this audit program, it is very important to place an emphasis on those parts of your company that are more important for your management system, and also on those with the biggest risks. For example, in an ISO 27001 audit you might focus on:

- the IT administrator, as the person responsible for implementation and maintenance of the technical controls related to information security,
- the customer database, as the most sensitive collection of information as identified by the risk assessment,
- the sales representatives, as employees who handle sensitive data (client information and prices),
- etc.

Also, you have to take into account previous audit results – if you performed audits for each of your 10 departments during the previous year, and department number 3 had the biggest number of nonconformities, then you might plan several audits for just this one department, or one audit that is more detailed than those used for the other departments.



**Documentation tip:** (mandatory) A document that describes a series of internal audits, usually called *internal audit program*.



---

## 3.5 Audit plan for an individual audit

---

ISO standards do not specify what you should write in your audit plan, but typically the following is included:

- A list of all the departments or other elements of the management system you are going to audit in this individual audit. Basically, you have the option to organize the audit **department by department**, or **process by process**, or **clause by clause of the standard** – for example, if you choose the clause-by-clause approach you might review the top-level policy first, followed by control of documented information, identification of legal requirements, etc.
- Timing for each of these items – for instance, you might plan to visit the Human Resources department at 9 AM, the production facility at 11 AM, etc.
- Contact persons for each of these items – this is important because this way, those people will be able to plan their time for you.
- If you have more than one auditor, then you should specify who the team leader is, and which auditor will audit what.
- Finally, you can copy the audit objectives, criteria, and method from the audit program.

As I mentioned earlier, the audit plan is not a mandatory document, but if you don't have much experience in auditing, or if you are planning to perform a rather complex audit, this kind of a document could prove to be quite useful.



**Documentation tip:** (non-mandatory) A document that describes the details of one audit, usually called the *internal audit plan*.

## 3.6 Success factors

---

In summary, if you want your internal audit to be organized properly, you have to do the following:

- Decide the best method for your company to use when organizing the internal audit.
- Although they are not all mandatory, write down the three key documents for the internal audit: internal audit procedure, annual audit program, and audit plan for each individual audit.

# 4

## STEPS IN THE INTERNAL AUDIT PROCESS

This chapter will guide you through the main activities that need to be performed in order to conduct a successful internal audit. All the steps – from document review to corrective action follow-up – will be explained in detail, and all these steps must be taken in order to conduct an effective internal audit.

### 4.1 Seven steps for performing the internal audit

---

The internal audit consists of the following seven elements or steps, which should be performed in this sequence:

1. **Document review** – in this step you should review all the policies and procedures and check whether they are compliant with your ISO standard; also, this step is crucial for creating the work documents (i.e., the checklist) in the next step.
2. Creation of the **internal audit checklist** – based on the insight from reading all the documentation, you should prepare your notes in the form of a checklist, which will help you remember what you need to do during the main audit.
3. Writing the **internal audit plan** – as explained in the previous chapter, the internal audit plan will help you plan the detailed timing, people you will talk to, and so on.
4. Conducting the **main audit** – this is the most important part of your internal audit, which you will have to perform on-site,

where the actual activities are taking place. During the main audit you'll need to talk to people, look for records, and observe whether everything is compliant with the standard, with the company documentation, and with other requirements.

5. Writing the **internal audit report** – in this step you have to document your audit findings.
6. Writing the **corrective action requests** – this is where you have to initiate the process of resolving the nonconformities you have found.
7. Conducting the **follow-up on corrective actions** – in this step you have to make sure all the nonconformities have actually been resolved.

As you probably noticed, these seven steps are logically related one to each other, and you'll have to perform all seven of them if you want your internal audit to be successful.

In this chapter I'll explain how to perform steps 1), 2), 5), 6), and 7). For details on writing the internal audit plan, please see the previous chapter, while the next chapter is dedicated to the main audit.

## 4.2 Performing document review

---

The purpose of the document review is twofold:

1. to check whether the policies, procedures, and other documentation are compliant with your ISO standard and other requirements from interested parties, and
2. to get to know the company better and prepare the audit checklist and the audit plan.

Basically it works like this: you have to take all the documents and read them one by one in some logical sequence, and determine whether all the requirements from the ISO standard and from interested parties are met. It

is also advisable to take some of the most important records, like list of legal, regulatory and contractual requirements; corrective actions; and management review minutes; and check them during this step. You should also check the most important records for particular management systems, e.g., incident log for the EMS and ISMS, and customer complaints for the QMS.

If you do not have much experience in auditing, the best option would be to read the documentation in the same sequence as the standard is written – start with the documents related to clause 4, then move on to documents related to clause 5, etc.

When you read the documentation, you have to take two types of notes:

- Notes about what you will need to check during the main audit – for example, check if authorized employees have access to particular reports, or check if the responsible person is performing specific trainings as prescribed by the company's training procedure – these notes should be part of your internal audit checklist.
- Notes about nonconformities – if you find that something is not compliant with the standard or with other requirements, you have to formalize these findings through the internal audit report.

You can perform the document review on-site, in the department you're auditing, or off-site in your own office; it doesn't really matter where you do it – both approaches are fine. If you need any explanations from the auditee, you can call the responsible person, so there is no need to be in the same location.

## **4.3 Creation of the internal audit checklist**

---

As mentioned before, the purpose of the internal audit checklist is to remind you of what you have to do during the main audit – the biggest problem during the main audit is that you'll have to speak to lots of people, look for

various types of evidence, think of various clauses of the standard, and have in mind many internal policies and procedures, and all of that is almost impossible without having some kind of a reminder.

As mentioned in the previous section, you'll create this checklist during the document review – as you are reading the internal documentation, learning what internal rules the company has and which records need to be produced, you must take notes on what you'll need to check. So, for example, check if all interviewees have access to the document management system where the entire documentation is stored, check if all the records are produced as prescribed by particular documents, etc.

So, obviously, such a checklist has many benefits; however, it also has its disadvantages – the biggest problem with a checklist is that it might drive you in one direction during the main audit and cause you to miss some newly discovered leads that haven't been planned for in your checklist. For example, while checking whether the corrective actions have been performed correctly, you might have heard that the top management did not invest enough resources into resolving the nonconformities, but because it wasn't on your checklist you didn't pursue that lead any further.

Therefore, when creating the checklist you have to remember that it is only a helping tool; it is not something you must follow 100%.

There are various approaches to writing the checklist, but probably the best one is where you use a document with four columns:

1. **Reference** – this would contain, e.g., the clause number of the standard, or section number of a policy, etc.
2. **What to look for** – this is where you write what it is you would be looking for during the main audit: whom to speak to, which questions to ask, which records to look for, which facilities to visit, which equipment to check, etc.
3. **Compliance** – this column you fill in during the main audit, and this is where you conclude whether the company has complied with the requirement. In most cases this will be Yes or No, but sometimes it might be Partially or Not Applicable.

4. **Findings** – this is the column where you write down what you have found during the main audit: names of persons you spoke to, quotes of what they said, IDs and content of records you examined, descriptions of facilities you visited, observations about the equipment you checked, etc.

In such a document you use only columns 1 and 2 for creating the checklist, while columns 3 and 4 are used during the main audit for recording the findings. In the following chapter I'll explain how to fill out columns 3 and 4.

Here's an example of an internal audit checklist that is focused on ISO 27001 clause 4.2 (Understanding the needs and expectations of interested parties); the data filled out in the third and fourth columns are only examples of what an internal auditor might write during the main audit.

Reference	What to look for	Compliance	Findings
ISO 27001 clause 4.2	Did the organization determine interested parties?	Yes	The company has listed all the interested parties in the "List of interested parties."
ISO 27001 clause 4.2	Does the list of all requirements from interested parties exist?	Partially	Only the laws and regulations are listed, but the requirements of partners and customers are not listed.

Figure: Example of internal audit checklist

During the document review you can also create some other work documents for your internal audit (e.g., forms in which you will collect the

information), but in most cases the internal audit checklist, in the form that is described above, will be enough.



**Documentation tip:** (non-mandatory) Informal notes made by the internal auditor, usually called the internal *audit checklist*.

## 4.4 Writing the internal audit report

---

The internal audit report is a mandatory document according to ISO standards, which is quite logical – how would you be able to communicate the results, if not in written form? More importantly, these results need to be remembered for at least a couple of years, so writing a report is the only way to do it.

Generally speaking, this report has three parts:

1. The general part where you have to fill out the dates, name(s) of the auditor(s), which part of the company you audited (audit scope), audit criteria, audit objectives, and other general information.
2. Audit findings – nonconformities you have found and your observations.
3. Audit conclusions – your general opinion on how much the company is compliant with the standard, and how well the management system fulfills its objectives.

The biggest part of this report will be a list of nonconformities and observations (see also section 2.5 for a general description), and the best way to describe the nonconformity is to write down these four elements for each nonconformity:

1. An exact reference to a clause of the standard or to the section



of a document against which you found the nonconformity – e.g., “ISO 9001 standard clause 7.2 d).”

2. A short description of the requirement that was not complied with – e.g., “The standard requires the existence of evidence of trainings.”
3. A description of what you have found – e.g., “The training records for induction trainings were not kept in the HR department, although those trainings were important for the QMS.”
4. An exact reference to the evidence – e.g., “HR department archive on February 12, 2017, did not contain any records on induction trainings.”

Observations are usually in a non-structured form: a couple of sentences where you describe what is good or what could be better will suffice – for example, “The QMS trainings could include more time for handling customer complaints because in some cases, the reaction to a complaint was not quick enough.”

You do not have to make this report too detailed, but it does need to be very precise.



**Documentation tip:** (mandatory) A document that describes the results of the internal audit – usually called the *internal audit report*.

## 4.5 Initiating corrective actions

---

Corrective action requests or reports (usually referred to as “CARs”) are a formal way to ask the company to resolve a nonconformity. These CARs are written based on the internal audit report, and in many cases they are written by the internal auditor – although it is not mandatory for the auditor to write them. Sometimes the corrective action requests will be written by

persons who are in charge of certain areas – for example, if a nonconformity related to training records is found, then the head of the HR department might write the CAR. Once you submit your internal audit report you should agree with your boss as to who should write the corrective action requests.

ISO standards require companies to establish a process for handling corrective actions (and write a procedure if they find it appropriate), so the internal auditor must write this corrective action request according to the established process/procedure in the company. In any case, such corrective action must define exactly who is in charge of resolving the nonconformity, the deadline, the cause, etc.



**Documentation tip:** (mandatory) Records that show what the nonconformities are in order to start the corrective actions, usually called the *Corrective Action Requests (CARs)*.

## 4.6 Corrective action follow-up

---

The internal audit job does not stop with writing the corrective action requests – internal auditor needs to make sure that nonconformities are really resolved.

This is done by looking at the corrective action form that should be filled out by the person who will complete the corrective action – these forms provide insight to the internal auditor on what has been done.

Using this information, the internal auditor needs to make sure that this particular corrective action has been performed, and if it has really resolved the root cause of the nonconformity. So, in fact, this follow-up will be a kind of small audit, focused only on this nonconformity – the internal auditor should use all the internal audit techniques; the only difference is that the scope in this follow-up will be smaller.

## 4.7 Success factors

---

In summary, to make your audit process succeed, take care of the following:

- Be careful not to skip any of the seven steps in the internal audit process.
- Thoroughly perform the document review to prepare yourself for the audit.
- Create your own internal audit checklist that will guide you throughout the main audit.
- Make your internal audit report short and precise.
- Initiate all the corrective actions to make sure that responsible persons will see them.
- Consider your job finished only after you verify that the corrective actions have been resolved.

# 5

## PERFORMING THE MAIN PART OF THE AUDIT

This chapter will explain how the on-site audit is to be performed: you'll learn about the most common mistakes the auditors make, as well as the techniques for finding evidence, how to sample the records during your audit, and how to record the evidence you gathered during your internal audit. And, at the end, you'll see the interviewing techniques and best practices for performing an on-site audit.

### 5.1 Making assumptions: The biggest auditor mistake

---

Having preconceptions and making assumptions is the biggest mistake an auditor could make. For instance, the auditor might expect that a company must have a documented procedure for corrective actions; however, ISO standards do not require such a procedure to be documented – ISO standards require that corrective actions should be a managed process. Therefore, regardless of whether a documented procedure exists in 90% of the companies, the auditor cannot demand that every company has it.

So, do not assume that something is required – you have to do your homework first, and determine what the real requirements are. And this is usually done in the document review phase.

Therefore, my main point is this: during the audit you have to keep an open mind – when you see something, at first sight it might seem wrong to you, or at least strange, but think twice before you raise a nonconformity. Just because something is different from what you usually see, doesn't mean that it does not comply with the requirements. In my auditing career, very often I've thought to myself: "How could the auditee make such a big

mistake?” – only to find out later that their solution was much better than the one I thought to be right.

## **5.2 Purpose of the opening meeting**

---

The opening meeting is a meeting between the auditor and the top management of the company, at the very beginning of the main audit. Its purpose is to ensure that the auditee clearly understands the audit objectives, timing, roles and responsibilities, outputs from the audit, etc.

This opening meeting is not mandatory for an internal audit (it is mandatory for a certification audit), and in most smaller companies it is usually not performed because the top management is already informed about the audit. However, in larger companies it might make sense to arrange this meeting, especially if the management of a department that is to be audited doesn't know much about it.

Besides providing a description of the audit process and other key features of the audit, the opening meeting is a good occasion to discuss whether an audit guide will be needed – an audit guide is a person who stays with the auditor the whole time, and takes the auditor through the company according to the audit plan and any requests by the auditor.

Obviously, an audit guide is very useful if the auditor doesn't know the company well, but if the internal auditor is a long-time employee who knows almost everything about the company, then this guide is not necessary.

## **5.3 Techniques for finding evidence during the on-site audit**

---

As mentioned before, the auditor's job is not guessing – he or she has to find evidence. There are basically three methods for finding evidence when performing the on-site audit:

1. reviewing records and documents,
2. interviewing the employees, and
3. observing the activities or facilities.

Let's see how to accomplish these...

**Reviewing the documents and records** is done by asking the auditee to provide them, and then reading them thoroughly. This is the best kind of evidence, so you should always look for it – in many cases you won't find documents, simply because they are not mandatory, but very often you will find records of some kind. So, for example, if you want to find out how the training process is done in a company, then you'll ask for their training procedure; if you want to find out which trainings have been done for a particular employee, you'll look for her training records. It doesn't matter if you don't know where those documents and records are located – you should ask the auditee to bring them to you, and it is their responsibility to find them.

If there are no records, then **interviewing the employees** is very often the only method to find out whether a process is carried out as required. Because speaking to only one person is not reliable enough to be solid proof, you should speak to a couple of employees who are part of the same process to see if their statements match. So, for example, if you ask a few employees how they handle electronic waste, and all of them give you the same or very similar answers, then this is proof that this process is done in a defined way; on the other hand, if you receive very different answers, then this would be proof that the process has not been defined, or that the employees are not trained for it.

In some cases, you will have to **observe the activities and/or facilities**, together with other methods (reading the documents and records, and interviewing the employees). For example, you might want to visit the server room to see how access control is implemented and how the facility is equipped. This way, you will find evidence showing whether the management of the server room is compliant with the procedures, and whether the procedures match the statements of the employees.

Later on I'll explain how to take records while you collect the evidence.

## **5.4 Sampling the records**

---

When reviewing the records, sometimes it is not possible to read them all. For example, if a company has 1000 employees, it wouldn't be possible for you to check the training records of each and every one of them; on the other hand, if a company has only 20 employees, then it is probably a good idea to check all their training records.

If it is not feasible to check all the records, you have to find those that are the most relevant – therefore, you should focus on those records that are the most important, or those where the possibility of finding a nonconformity is the biggest. So, for instance, if your company has thousands of employees and your most critical records are the ones containing personal data of your clients, then you should check primarily the training records of employees who are handling this kind of data; further, you should focus primarily on new employees' records because there is a higher chance that those employees are not properly trained when compared to employees who have been with the company for a longer period of time.

And another important tip: you shouldn't let the auditee provide you the records of their choice – the decision on which records to choose should be yours alone.

## **5.5 Recording the evidence during the audit**

---

The internal audit is one of the processes where records need to be produced. As mentioned before, the internal audit report is a mandatory document that has to be created as a consequence of performing the audit; however, such a report wouldn't be possible if you didn't write down all the evidence you found. The point is, during the audit you'll examine hundreds of documents and records, speak to dozens of people, visit several facilities – it is simply impossible to remember all of them.

Therefore, it is crucial to write down everything you see and hear. For documents, you should write down the exact name of the document together with its version number and date of publishing; for records, you should note the exact name of the record together with its date and serial number; for interviews, you should write down the name of the person you were speaking to, his job title, the date and time, and exact quotes that are relevant; for observation of facilities and processes, you should write down the exact rooms where these are located, the date and time, and the description of the items you noticed.

The best practice is to write all this evidence in the internal audit checklist I mentioned earlier, especially if you made that checklist in such a way that on the right-hand side you have all the items that need to be checked, and on the left-hand side the space where you write your findings.

Audio and video recording is not a common way of recording the evidence; neither is copying the documents and records, nor asking for written statements – as said earlier, you should keep your audit records accurately so as to be able to find this same piece of evidence later on if needed. Once you write the audit report, you should keep your records because they might be needed months, sometimes even years after the audit has been finished.

Of course, you need to keep all those records confidential – you might record some sensitive information, or someone’s opinion that might be unpleasant for other employees in the company. So, if protecting the confidentiality of audit records is not already addressed through the internal audit procedure or some other documents, make sure you discuss how to protect the audit records with someone from the top management.

## **5.6 Interviewing techniques for the audit**

---

Interviewing the people is probably the most difficult way to find the evidence, but at the same time, it’s the best way to find out how things are really done in a company.

First of all, how do you get people to start talking? To do this, you should use a technique called “open-ended questions” – for example, you should



ask: “Please describe to me how you control the access to your IT system,” or “Please describe how you decide which trainings should be provided to new employees.” This technique allows the auditee to start talking, and by doing so, to reveal lots of things about how the company operates – in reality, this is how you get most of your leads, or the things you need to check out because they might prove to have nonconformities. Probably the best open-ended question is: “Please describe what you do in the company.”

On the other hand, “closed-end questions” should be avoided – examples of such questions are: “Is your job title Office manager?” or “Is this the room where you store electronic waste?” – those closed-end questions can provide only Yes or No answers, and are not really helpful if you want to find out more about company operations.

There is one exception when closed-end questions are useful – this is when you want to confirm that you found evidence. For example, you might ask: “Are you sure that you didn’t send employee XYZ for training on personal data protection?” When you get a straight answer, this will be your evidence.

The second important thing is to find out the root cause of the problem – that is, why the nonconformity has happened. To achieve this, you can use the “Five Whys” technique. With Five Whys, you should ask the question “Why” as many times as necessary to find out why something has happened – quite often, you have to ask this question five times.

For example, you might have found the nonconformity where new employees are not provided the training for personal data protection. So, you should ask the auditee, in this case the Human Resources manager: “Why weren’t they sent for training?” And, she might answer, “Because we didn’t know they would be handling personal data.” Then you should ask: “Why didn’t you know this?” And, she could say, “Because their line manager didn’t tell us all the work they would be doing.” Then you should go to the line manager and ask him: “Why didn’t you provide this information to the Human Resources manager?” And, then he might answer, “I’m sorry, I simply forgot to include this part of the information when I sent the report to the HR department.” And, then you might ask: “Why is it possible that you could forget this piece of information?” And,

he might answer, “Actually, I don’t have a system that could remind me about what items I should include in my report.” And, finally, you might ask: “Don’t you have some kind of a checklist of all the information you need to send to the Human Resources department once you get a new employee?” And, he might answer, “No, we have no such checklist.” So, in this case the root cause of the problem is that there is no checklist of all the information needed.

## 5.7 Closing meeting

---

A closing meeting is typically scheduled at the end of the main audit, with the purpose of formal presentation of the audit findings. Most of this meeting should be about nonconformities that the auditor has found, and also about observations.

Similarly to the opening meeting, the closing meeting is not mandatory for internal audits and is not common for smaller companies; however, it might make sense in larger companies where the communication needs to be more formalized.

## 5.8 Success factors

---

To summarize, here is what you need to do to make your on-site audit successful:

- Avoid making any assumptions: be open to any new ideas.
- Make sure you use all three techniques for collecting evidence: documents and records, interviews, and observations.
- You must be the one to decide which records to look at, no one else.
- You should make a record of every detail you see, hear, or read during the audit – this will be your basis for writing the report.

- While interviewing people, you should ask open-ended questions.

# 6

## BONUS CHAPTER: DEVELOPING AN AUDITING CAREER

Some of you probably see auditing as a career opportunity – that is why I included this chapter, to show you how to move forward and become not only an internal auditor, but also lead auditor for certification bodies.

### 6.1 How to become a certification auditor

---

Many people think that just by attending the Lead Auditor Course for a particular ISO standard they have become a certification auditor. Well, this is not entirely true.

If you want to become a certification auditor and work for a certification body, here is what is required:

- 1) **Prior experience** – You need to have prior experience in a relevant industry; for example, for ISO 27001 you need to have at least four years of experience in information technology, of which at least two years is on a job related to information security.
- 2) **Pass the exam** – The Lead Auditor Course lasts five days, and on the fifth day you need to pass the written exam. Therefore, you need to invest considerable effort, not only by studying for the exam, but also by attending the full five days of the course (if you miss a single day, you will not be permitted to take the exam).
- 3) **Find a certification body** – You need to find a certification body that needs a certification auditor; that may prove to be a difficult task, because most of the certification bodies already have their auditors.
- 4) **Go through the trainee program** – When you find a certification

body that is interested, this doesn't mean you'll start auditing from the first day. First you have to go through a trainee program (or similar), during which you will attend real certification audits (done by more experienced colleagues) where you will learn how to perform such audits. Usually, this trainee period lasts 20 audit days, after which you'll be entitled to perform certification audits as part of the audit team.

- 5) **Gain audit experience** – To become the Lead Auditor, i.e., to lead a team of auditors performing certification audits, you need to have experience in at least three complete certification audits.

## 6.2 What do the Lead Auditor Course and Lead Implementer Course look like?

---

Both the Lead Auditor and Lead Implementer courses last for five days, and on the fifth day you have to pass an exam; both courses are quite intense, and normally you have to attend 40 hours in five days.

On the first day of the course, you will take a detailed look into each clause of the standard and a tutor will teach you how to interpret the standard, as well as the underlying logic. After this first day, the Lead Auditor course will focus mainly on auditing techniques of the particular standard, while the Lead Implementer course will explain the best methods for implementation.

Most of the courses are quite interactive – e.g., the courses I delivered had about 15 workshops during these five days, which gave students a perfect opportunity to learn while working as a team; of course, there are also lectures, and a good tutor will encourage discussion and applicability of the standard to real situations.

You do not need any special knowledge to enroll in the course – if you go for the ISO 27001 course, it is enough to have average knowledge of IT, and no prior knowledge of information security is needed.

## 6.3 Lead Auditor Course vs. Lead Implementer Course – Which one to go for?

---

**The main differences.** Lead Auditor courses can (and should) be accredited (i.e., a third party has verified that the course provider has developed and delivered the course in a satisfactory way), while the accreditation for the Lead Implementer course is not that important.

However, the main difference between these two courses is in their focus. If you want to focus your career on auditing, you should definitely go for the Lead Auditor course; if you are a practitioner who is focused on implementation, you should go for the Lead Implementer course. If you are in a consulting business, you should probably go for both, because this is how you'll learn not only the implementation techniques, but also the certification auditor's criteria; not to mention that the more certificates you have as a consultant, the more valuable you are.

**Which training provider to choose?** These courses are usually provided by the certification bodies, but specialized training organizations also deliver them. You should just search the Internet for the certification bodies in your country, and chances are that you'll find such courses locally.

When choosing a training provider, you should look for Lead Auditor courses that are accredited by IRCA, Exemplar Global, or PECB – this means that, once you pass the exam, this certificate will be accepted by any certification body if you choose to work as lead auditor for them.

Accreditations for Lead Implementer courses are not that widespread, so your first criteria when choosing a course should be the tutor – if this person has a good reputation, chances are you will attend a high-quality course.

**Invest time in your education.** Being absent from work for five whole days may sound inconceivable to you, so if you do not see ISO standards as your career opportunity, you should go for one- or two-day courses.

However, if you seriously plan to have a career in ISO standards, these five days will be a crucial investment for you. Believe me, not only will you get the certificate (which is a must if you want others to recognize you), but

you will also learn the essence of these standards – something you won't be able to do just by reading the standard from time to time.

# 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





# **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.