ISO 27001 ANNEX A CONTROLS IN PLAIN ENGLISH

ISO POCKET BOOK SERIES

02

A Step-by-Step Handbook for
Information Security Practitioners in Small Businesses

DEJAN KOSUTIC

ISO 27001 Annex A Controls in Plain English

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

Dejan Kosutic

ISO 27001 Annex A Controls in Plain English

Step-by-step handbook for information security practitioners in small businesses

Advisera Expert Solutions Ltd
Zagreb, Croatia

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

ISBN: 978-953-57452-9-7

First Edition, 2016

ABOUT THE AUTHOR

Dejan Kosutic is the author of numerous articles, video tutorials, documentation templates, webinars, and courses about information security and business continuity management. 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.

Click here to see his LinkedIn profile

TABLE OF CONTENTS

PREFACE

When my book *Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own* was published earlier this year, I soon realized that many people were reading it because they were interested to learn about security controls (safeguards) that are listed in ISO 27001.

Therefore, I have created this shorter book, a part of the pocketbook series, which is focused solely on the 114 controls from the ISO 27001 Annex A. This book, *ISO 27001 Annex A Controls in Plain English*, is actually an excerpt from *Secure & Simple*, and has been edited with only a few smaller details. So, if you compare the sections from *Secure & Simple* that speak about Annex A controls, you'll see the same sections here, with basically the same text.

So, why have another book with almost the same text? Because I wanted to provide a quick read for people who are focused solely on safeguards, and don't have the time (or need) to read a comprehensive book about ISO 27001, i.e., a book like *Secure & Simple*.

Another benefit is that this book has all the sections about Annex A controls placed in sequential, continuous form, whereas in *Secure & Simple,* these sections are scattered throughout a couple of chapters.

You might also be puzzled by the fact that this book is rather short, whereas there are other books on ISO 27001 safeguards on the market that are much more lengthy and detailed. Is it really possible to explain such a complex subject in a short book like this? Well, there are two answers for this:

First, this book gives only an overview of each control, and it doesn't provide detailed guidelines – for that purpose you'll find many links in the book that show you the relevant articles you can read on the Advisera.com website. Second, you'll find the best guidelines on how to implement each control from ISO 27001 Annex A in the ISO 27002 standard.

So, the purpose of this book is to open a door for you into the world of security controls – it will explain why they are important, how they are structured, how they are selected, how they are related to security management, and finally, the purpose of each control. Once you pick the controls you are particularly interested in, you will know what to search for further, and where to search.

ACKNOWLEDGMENTS

Special thanks to Ana Meskovska, who helped me with the descriptions of Annex A controls.

1
INTRODUCTION

Why are these security controls important, and why are they listed in Annex A of ISO 27001? How are they related to risk assessment?

And, is this book the right choice for you?

1.1 Who should read this book?

This book is written primarily for beginners in ISO 27001 and for people with moderate knowledge about security controls (i.e., safeguards) – I structured this book in such a way that someone with no prior experience or knowledge about information security can quickly understand what they are all about; however, if you do have experience with ISO 27001, but feel that you still have gaps in your knowledge, you'll also find this book very helpful.

This book provides an overview of the structure of ISO 27001 Annex A, as well as of the 114 controls that are found in this Annex, and what they mean for smaller and medium-sized organizations (i.e., companies with up to 500 employees). All the principles described here are also applicable to larger organizations, so if you work for a larger company you might find this book useful; however, please be aware that you will have to use more complex methodology – for example, for doing the backup, both the rules and the technology for it will be more complex than for a smaller company.

So, if you are an IT administrator, information security professional, or head of an IT department, or a project manager

tasked with implementing security controls in a small or mid-sized company, this book is perfect for you to start understanding this subject.

So, to conclude, this book gives a systematic picture of what ISO 27001 Annex A is all about, and gives an overview of all the controls that are included in this Annex A. It is true that this book doesn't go into details of each and every control, but for that purpose you'll find many links in this book to articles that will explain the details you're interested in.

1.2 What this book is not

This book is focused on what is the purpose of individual controls and how to manage them; it is not focused on which technology you should be using for particular control. For example, this book will outline what principles are important for doing the backup, but the book doesn't provide you with guidelines on which technology you should purchase.

This book won't give you finished templates for all your policies, procedures, and plans; however, this book will explain to you how to structure the documents, which options you have for writing such documents, and who should be involved in writing and decision making related to each document.

This book is not a copy of ISO 27001 and ISO 27002 standards – you cannot replace reading these standards by reading this book. This book is intended to explain how to interpret the standards (since the standards are written in a rather unfriendly way); however, this book is not a replacement for ISO 27001 nor ISO 27002 – indeed, for detailed guidelines on each and every control from ISO 27001 Annex A you should read ISO 27002 standard.

So, please don't make the mistake of starting an implementation without actually reading ISO 27001 and potentially ISO 27002 – I think you'll find ISO 27001 and ISO 27002 together with this book to be the perfect combination for your future work.

1.3 ISO 27001 vs. ISO 27002

If you had the chance to read both the ISO 27001 and ISO 27002 standards, you probably noticed that ISO 27002 is much more detailed, much more precise – so, what's the purpose of ISO 27001 then?

First of all, a company cannot get certified against ISO 27002 because this is not a management standard. In other words, ISO 27002 focuses only on security controls, but it doesn't explain how to build an Information Security Management System, which would include roles and responsibilities, setting the objectives, risk management, internal audits, etc. Therefore, certification against ISO 27002 is not possible.

The controls in ISO 27002 are named the same as in Annex A of ISO 27001 – for instance, in ISO 27002 control 6.1.3 is named Contact with authorities, while in ISO 27001 it is A.6.1.3 Contact with authorities. But, the difference is in the level of detail – on average, ISO 27002 explains one control on one whole page, while ISO 27001 dedicates only one sentence to each control.

Finally, the difference is that ISO 27002 does not make a distinction between which controls are applicable to a particular company, and which are not. On the other hand, ISO 27001 prescribes a risk assessment to be performed in order to identify for each control whether it is required to decrease the risks, and if it is, to which extent it should be applied.

Now, the question arises: why is it that those two standards are published separately; why haven't they been merged, bringing together the positive sides of both standards? The answer is usability – if it was a single standard, it would be too complex and too large for practical use.

To conclude, ISO 27002 is a very good additional standard where you can learn how to implement individual controls from ISO 27001; however, ISO 27002 should not be used without ISO 27001 because this would lead to an isolated effort of a few information security enthusiasts, with no acceptance from the top management and, therefore, with no real impact on the organization.

1.4 The crucial link between risk management and security controls

When speaking with someone new to ISO 27001, very often I encounter the same problem: this person thinks the standard will describe in detail everything they need to do – for example, how often they will need to perform backup, how distant their disaster recovery site should be, or even worse, which kind of technology they must use for network protection or how they have to configure the router.

But, the fact is ISO 27001 does not prescribe these things; it works in a completely different way.

Why is ISO 27001 not prescriptive? Let's imagine that the standard prescribes that you need to perform a backup every 24 hours – is this the right measure for you? It might be, but believe me, many companies nowadays will find this insufficient – the rate of change of their data is so quick that they need to do backup if not in real time, then at least every hour. On the other hand, there are still some companies that would find the

once-a-day backup too often – their rate of change is still very slow, so performing backup so often would be overkill.

The point is – if this standard is to fit any type of a company, then this prescriptive approach is not possible. So, it is simply impossible not only to define the backup frequency, but also which technology to use, how to configure each device, etc.

By the way, this perception that ISO 27001 will prescribe everything is the biggest generator of myths about ISO 27001.

So, you might wonder, "Why would I need a standard that doesn't tell me anything concretely?" Because ISO 27001 gives you a framework for you to decide on appropriate protection. The same way, e.g., you cannot copy a marketing campaign of another company to your own, this same principle is valid for information security – you need to tailor it to your specific needs.

Risk management is the central idea of ISO 27001. And, the way ISO 27001 tells you to achieve this tailor-made suit is to perform risk assessment and risk treatment. This is nothing but a systematic overview of the bad things that can happen to you (assessing the risks), and then deciding which safeguards to implement to prevent those bad things from happening (treating the risks).

Requirements of interested parties. These requirements are a second crucial input when selecting the safeguards. Interested parties could be government agencies, your clients, partners, etc. – all of them probably expect you to protect the information, and this is reflected in the laws and contracts you have with them. Therefore, your safeguards have to comply with all these requirements as well.

The whole idea here is that you should implement only those safeguards (controls) that are required because of the risks and

requirements of interested parties, not those that someone thinks are fancy; but, this logic also means that you should implement all the controls that are required because of the risks or because of these requirements, and that you cannot exclude some simply because you don't like them.

IT alone is not enough to protect the information. If you work in the IT department, you are probably aware that most of the incidents are happening not because the computers broke down, but because the users from the business side of the organization are using the information systems in the wrong way.

And, such wrongdoings cannot be prevented with technical safeguards only – what is also needed are clear policies and procedures, training and awareness, legal protection, discipline measures, etc. Real-life experience has proven that the more diverse safeguards are applied, the higher level of security is achieved.

And, when you take into account that not all the sensitive information is in digital form (you probably still have papers with confidential information on them), the conclusion is that IT safeguards are not enough, and that the IT department, although very important in an information security project, cannot run this kind of project alone.

This fact that IT security is not enough for implementing information security is recognized in ISO 27001 – this standard tells you how to run the information security implementation as a company-wide project where not only IT, but also the business side of the organization, must take part.

1.5 Information security vs. IT security

One would think that IT security and information security are synonyms – after all, isn't information security all about computers?

Not really. The basic point is this – you might have perfect IT security safeguards, but only one malicious act done by, for instance, an administrator can bring the whole IT system down. This risk has nothing to do with computers; it has to do with people, processes, supervision, etc.

Further, important information might not even be in digital form; it can also be in paper form – for instance, an important contract signed with the largest client, personal notes made on a paper notepad by the CEO, or printed administrator passwords stored in a safe.

Therefore, I always like to say to my clients – IT security is only half of information security, because information security also includes physical security, human resources management, legal protection, organization, processes etc. The purpose of information security is to build a system that takes into account all possible risks to the security of information (IT or non-IT related), and implements comprehensive controls that reduce all kinds of unacceptable risks.

ISO 27001 enables this integrated approach to the security of information: as mentioned before, it requires risk assessment to be done on all of the organization's assets – including hardware, software, documentation, people, suppliers, partners, etc., and to choose applicable controls for decreasing those risks. When analyzing Annex A of ISO 27001, it turns out that only 37% of those controls are IT related – all the others are non-IT controls.

What does all this mean in terms of information security / ISO 27001 implementation? This kind of project should not be

viewed as an IT project, because as such it is likely that not all parts of the organization would be willing to participate in it. It should be viewed as an enterprise-wide project, where relevant people from all business units should take part: top management, IT personnel, legal experts, human resource managers, physical security staff, the business side of the organization, etc. Without such an approach you will end up working on IT security, and that will not protect you from the biggest risks.

1.6 ISO 27001 puts it all together

What I like about ISO 27001 is that it has this comprehensive, and at the same time, balanced approach to building up an information security management system (ISMS) – it not only gives a perfect balance between the IT and business sides of the organization, it also requires the direct involvement of top management in the information security implementation, ensuring that such project not only has all the required resources, but that it also supports the strategic objectives of the company.

ISO 27001 explains how to structure the information security documentation, but also how to apply only those security controls (safeguards) that are really necessary for the company. It gives you the tools to permanently review the whole system and improve it whenever it is possible; it provides you with a system on how to train your employees and make them aware of the importance of information security; it includes the requirements on how to plan the resources, including financial resources.

It also gives a perfect implementation path – it is written in such a sequential way that you just have to follow the structure of the standard to implement your ISMS in the most logical way.

Finally, it provides a management framework on how to evaluate whether information security has achieved some business value – by setting objectives and measuring whether these objectives are fulfilled. You may be surprised, but I like this part very much – this is because if the management sees concrete benefits from their information security investment, it is the best way to ensure the long and successful life of the ISMS in your company.

1.7 Additional resources

Here are some resources that will help you, together with this book, to learn about ISO 27001 risk management and how to implement it:

- **ISO 27001 online courses** – free online courses that will teach you the basics of security controls in ISO 27001
- **ISO 27001 free downloads** – collection of white papers, checklists, diagrams, templates, etc.
- **ISO 27001 tools** – couple of free tools like Return on Security Investment Calculator, Implementation Duration Calculator, and Gap Analysis Tool.
- **ISO 27001 Documentation Toolkit** – set of all the documentation templates that are required for ISO 27001 implementation, including the policies and procedures for Annex A
- **Expert Advice Community** – a forum where you can ask a question on security controls (or any other ISO-related topic) and get the answers from leading experts
- **Official ISO webpage about ISO 27001** – here you can purchase an official version of ISO 27001 and ISO 27002.

2
OVERVIEW OF ANNEX A CONTROLS

In this chapter I'm not going to give you a detailed explanation of each and every control – but, if I were to do it, I wouldn't be speaking about ISO 27001 anymore; I would be explaining ISO 27002.

And, there is really no point in explaining the details of each control when you already have this covered in ISO 27002 itself – therefore, I'll give you an overview of which controls exist, how they are structured, and where they should be used; I also provided links to free materials that give you tips on the implementation, since those materials are so numerous that it would be difficult to include all of them in this book.

2.1 Introduction to ISO 27001 Annex A

Annex A of ISO 27001 provides a catalogue of 114 security controls grouped into 14 sections. These sections are divided into several sub-sections with different objectives. For example, the section A.12 Operations security has seven sub-sections. The third sub-section is A.12.3 Backup, and its objective is to protect against loss of data, and the fifth sub-section is A.13.5 Control of operational software, and its objective is to ensure the integrity of operational systems.

As I mentioned previously, not all of these 114 controls are mandatory – through the risk management process, a company can choose for itself which controls it finds applicable and then

it must implement them (in most cases, at least 90% of the controls are applicable).

The best thing about Annex A is that it gives you a perfect overview of which controls you can apply so that you don't forget some controls that would be important, and it gives you the flexibility to choose only the ones you find applicable to your business so that you don't have to waste resources on the ones that are not relevant to you.

The controls from Annex A can be organizational or technical, meaning they can be implemented by documenting policies and procedures, or by applying some technical means like installing anti-virus software or firewall, etc.

The truth is that Annex A of ISO 27001 does not give too much detail about each control. There is usually one sentence for each control, which gives you an idea on what you need to achieve, but not how to do it. More details about these controls are given in ISO 27002. This ISO 27002 has exactly the same structure as ISO 27001 Annex A, but with more detailed explanation on how to implement the corresponding controls. It is important to note here that it would be a mistake to use only ISO 27002 for managing your information security, since it does not give you any clues as to how to select which controls to implement, how to measure them, how to assign responsibilities, etc. ISO 27002 is best used as a supplementary standard to ISO 27001.

2.2 Structure of Annex A

As explained earlier, each section of Annex A covers controls related to a specific topic, such as controls for managing suppliers or controlling access. This kind of structure enables the users of this standard to understand what kinds of controls exist, and helps them to find the appropriate control quickly.

Let us have a quick overview of the purpose of the 14 sections from Annex A:

- **A.5 Information security policies** – controls on how the policies are written and reviewed
- **A.6 Organization of information security** – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking
- **A.7 Human resources security** – controls prior to employment, during, and after the employment
- **A.8 Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling
- **A.9 Access control** – controls for the Access Control Policy, user access management, system and application access control, and user responsibilities
- **A.10 Cryptography** – controls related to encryption and key management
- **A.11 Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.
- **A.12 Operational security** – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
- **A.13 Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.

- **A.14 System acquisition, development and maintenance** – controls defining security requirements and security in development and support processes
- **A.15 Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers
- **A.16 Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
- **A.17 Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
- **A.18 Compliance** – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

As you can notice from the presented structure of Annex A, the information security controls are not only IT related. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.

A more detailed overview of all these sections and their controls will be covered in the next sections.

2.3 Structuring the documentation for Annex A

Before starting to structure your documentation, let me repeat a couple of very important rules: you cannot simply start to select the controls and/or write the documents that you like the most

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

BIBLIOGRAPHY

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

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

ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

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

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management

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

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

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

http://training.advisera.com/course/iso-27001-foundations-course/ *ISO 27001 Foundations Course*, Advisera.com

INDEX

ISO 27001 Annex A Controls in Plain English

Step-by-step handbook for information security practitioners in small businesses

Think and act like a consultant with this comprehensive and practical overview of 114 security controls listed in Annex A of ISO 27001.

Author and experienced information security consultant Dejan Kosutic shares all his knowledge and practical wisdom with you in one invaluable book.

- ✓ Get a simple explanation how the Annex A is structured and which controls are included
- ✓ Understand what is the purpose of each control
- ✓ Learn how to structure policies and procedures for Annex A controls
- ✓ Get links to additional resources which explain controls in more detail
- ✓ All this, and much more…

Written in plain English and avoiding the technical jargon, *ISO 27001 Annex A Controls in Plain English* is written for normal people in plain, simple language. Whether you're an information security practitioner or new to the field, it's the right book to start learning about the subject.