PRACTICAL SUPPORT FOR IMPLEMENTING AND IMPROVING YOUR ISMS

NICO BASTEN

BETWEEN THE LINES ISO 27001

What's not written — but you need to know

Publishing house Trespaises

NICO BASTEN

BETWEEN THE LINES ISO 27001

What's not written — but you need to know

Publishing house:	Trespaises
ISBN:	9789090412764
BISAC:	COM032000 / BUS087000 / BUS097000 / COM046000
Version:	20251215
Keyword:	Information security

Design:	Astrid Honcoop
Cover:	Astrid Honcoop
Images:	Nico Basten
Printing and binding:	Amazon (International) and Pumbo (Netherlands)
Author photo:	Nico Basten

TABLE OF CONTENTS

ACKNOWLEDGMENTS

No one ever writes a book alone. While my name is on the cover, many others have contributed directly or indirectly along the way.

First, I would like to thank my clients, colleagues, peers, and auditors I've had the privilege to work with over the years. Your challenges, ideas, questions — and sometimes frustrations — were the inspiration behind the practical examples, pitfalls, and tips in these pages. You've shown me how ISO 27001 works in the real world, and occasionally how it doesn't.

A special thanks goes to my two technical reviewers; Cees van der Wens and Gerrit-Jan Spruijt. Your critical perspective and our discussions were invaluable in sharpening my thinking. We didn't always see eye to eye, but that's part of the craft. Your feedback made this book stronger.

I also want to thank you, the reader. By picking up this book, you show you're willing to look beyond the standard itself. My hope is that the knowledge, examples, and tools here not only help you understand ISO 27001 but also make working with it more enjoyable.

Of course, I'm deeply grateful to my wife, Lizzy — for your patience in the Netherlands, Spain, and Suriname alike. You reminded me to come back to the present whenever I was lost in thought behind my laptop. And it was fun, useful, and refreshing to occasionally spar over this tough subject with someone who views it from just the right distance.

ally, a word of gratitude to four people who supported me throughout the writing process. As this was my first book, I was especially glad to have your help:

Perdiep Ramesar, of Het Schrijvershuis — my coach and guide on this journey. You kept the “moving train” on track, shared valuable tips, and helped me adjust course when needed.

Astrid Honcoop, of Het Ontwerploket — responsible for the design. The result is sleek and professional, and I’m proud of it.

Joanna and Judith, of Bookhelpline.nl, for your meticulous work in ensuring the English translation is perfectly accurate.

FOREWORD

When Nico asked me to write the foreword to his book, I felt both honored and curious, as the subject is essential to building secure information security practices.

In my role as Country Head Director of Internal Audit at an international bank, I see every day how crucial it is that information security is not treated as an abstract concept, but as an integral part of business operations. ISO 27001 provides a powerful framework for this. It is more than just a standard; it is a foundation for trust.

This book is a practical guide for anyone looking to bridge the gap between policy and reality. Whether you are starting an implementation or aiming to raise the bar, it offers insights that truly matter.

Security is not a destination but an ongoing journey. My hope is that Nico's book will inspire you to continue that journey with conviction and vision.

Marlon Jodhabier RE

Group Audit Country Head Director at Deutsche Bank, covering the Netherlands, Luxembourg, France, Sweden, and Portugal

This foreword was written in a personal capacity and reflects my own views.

INTRODUCTION

It was over twenty-five years ago, in early 1998, that I took on my first role in information security: security officer at a pension fund company. Around the same time, I began my IT auditing studies at Erasmus University in Rotterdam. The field was still in its infancy, and I was fascinated by the concept of security awareness. That's why I chose it as the subject of my graduation thesis.

My conviction then — and still today — is that a positive security culture is a prerequisite for effective information security. Everyone needs to understand their role, tasks, and responsibilities, and act accordingly. This is part of governance, but I like to call it the chessboard.

It should come as no surprise that information security has become increasingly prominent in business. Threats are growing, as is the complexity of the IT landscape. Legacy systems — *the monsters in the basement* — now have to coexist with modern cloud applications. Artificial intelligence is pushing its way in, bringing both opportunities and risks, while organizations focus on their core business. As a result, supply chains are expanding rapidly. But do they still know exactly where and by whom security measures are applied—and what agreements are in place?

Beyond the growing (cyber) threats and complexity, laws, regulations, and accountability requirements are also increasing. Organizations are struggling with NIS2, GDPR, DORA, ISO 27001, ISAE 3402, SOC 2, and more. How can we be sure we comply with all these requirements? Can we demonstrate our compliance transparently to customers or regulators who ask for it? And can we still compete in tenders if we can't check the box for "ISO 27001 certified?"

The developments described earlier have had a major impact on the popularity of ISO 27001. It is a relatively concise document with a straightforward structure and an annex containing the most common security controls. This has made ISO 27001 the benchmark for organizations to demonstrate that they recognize the importance of information security and are committed to making it effective.

Over the past 25 years, ISO 27001 has evolved through several new versions. The main focus has been on further developing the management system — the Plan—Do—Check—Act cycle — and aligning it with other ISO standards such as ISO 9001 and ISO 14001.

For clarity: ISO 27001 consists of two parts. The first part covers chapters 4 through 10, which define the Information Security Management System (ISMS). The second part is Annex A, which contains ninety-three security controls.

The growing importance of information security and ISO 27001 has attracted a large number of professionals to the field. Yet despite this development, there is still a shortage of qualified specialists. CISOs, security officers, security managers, and vCISOs (virtual CISOs) are in constant demand. On the auditor side as well, there is no shortage of work, with certification bodies seeing many new entrants — and plenty of vacancies.

It is therefore no surprise that there are so many different interpretations of the standard's requirements. We are all people with our own mix of expertise, opinions, and preferences. ISO 27001 prescribes *what* must be done, but not *how* it should be achieved. Organizations need to interpret the requirements themselves and apply them in a way that fits their own context.

In recent years, I have supported a wide range of organizations — large and small, across different industries — with their ISO 27001 implementation and preparation for certification. Along the way, I have witnessed many discussions between CISOs and auditors about side issues and personal opinions of the auditor. Yet the real focus should be on the requirements of the standard and how the organization has applied them.

This book is primarily intended to strengthen security professionals. On the one hand, in discussions with their own executives, to convince them of the importance of having an ISMS. On the other, in conversations with management and staff, to enable meaningful discussions about the reasons behind security measures. And not least in discussions with auditors, to have constructive exchanges about the intent behind the ISO 27001 requirements.

Use this book as a complement to other professional literature — to stay sharp, to foster open dialogue, and to develop your own perspective.

The content of this book can be valuable for organizations at the start of an ISO 27001 implementation. The tips and templates can help ensure the ISMS is set up properly and delivers immediate added value. For organizations that have recently been certified, the content can also support a re-evaluation of certain principles and the optimization of the ISMS.

Like an old clock, an ISMS needs time to settle in, which is how continuous improvement is achieved — the essence of the PDCA cycle.

Like everyone else, I bring my own experience, expertise, opinions, and preferences. I still learn something new every day — from my clients, from auditors, and from other specialists in my network. This book was written in a personal capacity, and I am well aware that some peers may view certain topics differently — and that is perfectly fine. All interpretations, examples, and tips and tricks are drawn from my own experience and daily practice.

It remains essential to apply common sense when implementing ISO 27001. The content of this book can, of course, contribute to shaping ideas and supporting decision-making within your own organization. It does not aim to be exhaustive, nor does it treat every subject with the same level of depth. Instead, it is a collection of insights, with a focus on practical matters that I consider valuable.

In this book, I focus on what is not explicitly written in the standard. This is *ISO 27001 Between the Lines.*

The title was chosen deliberately, and it may well be the very reason I felt compelled to write this book. ISO 27001 leaves a great deal of room for interpretation, which — let's put it gently — does not always line up seamlessly. Yet it is precisely between the lines of this standard that the nuance lies. That is where the space is. Use this space to shape ISO 27001 around your organization, rather than forcing your organization to bend around the standard. Don't just jump through the auditor's hoops; put your own needs at the center so your ISMS fits like a comfortable coat.

Part 1 of this book explores in detail the challenges and solutions involved in ISO 27001 implementation and certification.

Part 2 focuses on the Information Security Management System (ISMS). At the end of each section of the standard, you will find a practical checklist to help you verify that nothing has been overlooked.

Part 3 provides guidance on managing externally provided processes, products, or services that are relevant to the ISMS. For many organizations, this is a current and complex topic, subject to both legal and regulatory requirements as well as contractual obligations.

Finally, the appendix of this book contains a complete overview of all checklists from Part 2.

For practical reasons, the term "he" is used throughout this book. However, this can equally be read as "she" or "they."

At the time of writing, ISO/IEC 27001:2022 was the most current version. For readability, this book refers to the standard simply as "ISO 27001," or "the standard."

Finally, this book focuses primarily on the first part of ISO 27001: the ISMS, described in Chapters 4 through 10. Various controls from Annex A are used as examples, but not all ninety-three are discussed in detail. Perhaps that could be the subject of another book in the Between the Lines series? I would be glad to

hear if there is interest. And of course, I also welcome any questions or feedback you may have in response to this book:
nico.basten@awaretoday.nl

I hope you enjoy reading this book.

Nico

BETWEEN THE LINES ISO 27001

ISO 27001 is immensely popular — and understandably so. Information security is complex, and threats continue to evolve. ISO 27001 helps make this landscape transparent and manageable for organizations that collaborate and seek clarity and assurance.

However, this popularity has also led to misunderstandings, differing interpretations, and ongoing discussions about what the standard actually requires. Too often, implementations focus primarily on satisfying auditors instead of creating real value for the organization. That is unfortunate — and unnecessary.

This book is a practical guide for anyone involved in organizing or assessing information security. It is for those who seek nuance and flexibility between the lines. Packed with anecdotes, real-world examples, pitfalls, tips, and useful templates, it offers guidance both to organizations just beginning their ISO 27001 journey and to those already certified who want to further refine their approach.

ABOUT NICO BASTEN

Nico Basten RE CISA CISSP has worked in the business world for more than forty years. He began his career in 1985 as a COBOL programmer and has since held various roles in system development, IT operations, IT audit, risk management, and information security. He has delivered ISO 27001 training for many years and has guided numerous implementations for both small and large organizations. Nico was born in 1964, lives in the Netherlands (Amersfoort) with his wife, and has two daughters and four grandchildren.

ISBN 9789090412764