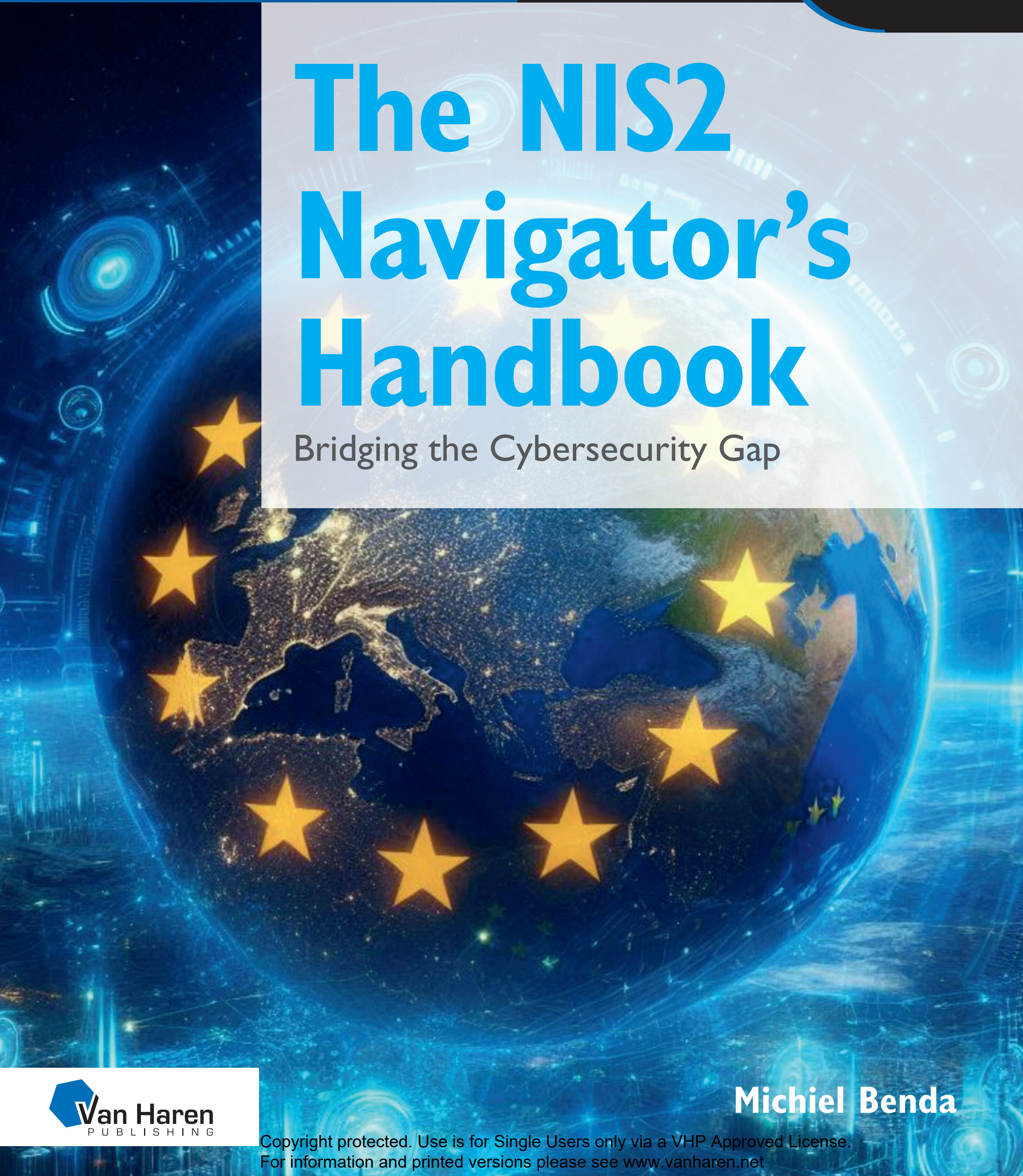
BEST PRACTICE

The NIS2 Navigator's Handbook

Bridging the Cybersecurity Gap



Michiel Benda

Van Haren PUBLISHING

The NIS2 Navigator’s Handbook

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business Management and
- Project Management

Van Haren Publishing is also publishing on behalf of leading organizations and companies: BRMI, CA, Centre Henri Tudor, CATS CM, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CMMI®
COBIT®
e-CF
ISM
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
NIS2
SABSA
SAF
SIAM™
TRIM
VeriSM™
XLA®

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Project Management

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

Business Management

BABOK® Guide
BIAN®
BiSL® and BiSL® Next
BRMBOK™
BTF
CATS CM®
DID®
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

For the latest information on VHP publications, visit our website: www.vanharen.net.

The NIS2 Navigator's Handbook

Bridging the Cybersecurity Gap

Michiel Benda

Van Haren
PUBLISHING

Colophon

Title:	The NIS2 Navigator's Handbook
Subtitle:	Bridging the Cybersecurity Gap
Series:	Best Practice
Author:	Michiel Benda
Reviewers:	Ite van Aardenne (Intergamma), Geert Antheunis (Cronos), Hendrik Decroos (Infosentry), Ulf Feger (Arlanxco Deutschland), Paul Gooijen (Mosadex Groep), Joran Leenders (Ypto)
Publisher:	Van Haren Publishing, 's-Hertogenbosch-NL www.vanharen.net
Lay-out and DTP:	Coco Bookmedia, Amersfoort-NL
ISBN Hard copy:	978 94 018 1227 6
ISBN eBook (pdf):	978 94 018 1228 3
ISBN ePub:	978 94 018 1229 0
Edition:	First edition, first impression, September 2024
Copyright:	Van Haren Publishing, 2024

The GAP analysis described in this book is available as a download. Use this QR code:

Although this publication has been composed with most care, neither author nor publisher can accept any liability for damage caused by possible errors and/or incompleteness in this publication.

Foreword

In 1881 a document called the Bhakshali manuscript was discovered by a farmer in India. It was carbon dated to be from around the 3rd or 4th century CE. What makes the manuscript particularly interesting is that it shows the use of the number 0 (zero) as more than a placeholder, but rather as a mathematical tool. It is said to be one of the greatest breakthroughs in mathematical history. Yet, while the whole world uses the zero nowadays as an indispensable basis for anything mathematical, recognition for this breakthrough and the person responsible for it seem to have been lost to time. The digital era in which we find ourselves is essentially based on the simple premise of zero and one. You could argue that, thanks to this Indian breakthrough, we now have a digital world. Because we have a digital world, we now have cyberspace, and because of cyberspace we are now faced with the Directive that this book is all about, NIS2. In short, I owe the fact that I am writing this book to a long forgotten Indian genius who decided that a zero should be used in mathematical calculations.

Grateful as I am for the zero, the fact that you are now reading this is because I have the support of many people around me who believe in what I do. In 2022, when it became clear that NIS2 was going to impact a lot of organizations, I was talking to the staff at TSTC, a security training institute in the Netherlands. I work with them to provide training on several security management topics. In our talks, we agreed that NIS2 would receive a lot of attention in many organizations operating in the European Union. These organizations would need to be trained so that they could ensure their compliance with the Directive and ultimately the laws in each of the Member States. I decided to build a training course that would cover NIS2 and the subsequent requirements that organizations would face. Instead of addressing the Directive from a technical and security perspective, I focused the training on business needs and requirements aimed at the management bodies of organizations. NIS2 makes it explicit that management bodies must be trained in cybersecurity which, for obvious reasons, should be a training course that addresses cybersecurity in the context of business operations. A training course for management bodies must deliver value beyond the understanding of a Directive. After all, management bodies are there to govern. The delivered value is to help them govern, and what better way is there than to provide them with a clear insight into the areas of cybersecurity in their own organizations that require improvement. This led to the creation of a GAP assessment tool that they could use during the training to gain an understanding of the requirements. At the same time, the tool would also give them an understanding of their own compliance and what to do to become compliant in areas that require improvement.

I started writing the training and the tool in the spring of 2023. The first step was coming to terms with the complexity of the Directive itself. The multitude of references to articles in other legislations makes it difficult to read. To give you an idea, I counted 90 different references to provisions and recitals in different treaties, laws, regulations, recommendations, and directives. The next step was to place the 46 NIS2 articles in relation to the 144 recitals it contains, thereby identifying what NIS2 expects organizations to do. Only then did the true writing start.

It has been an impressive journey. I have learned a lot about NIS2, but also about a wide variety of other topics. The most surprising outcome for me was that I started putting together a training course and I ended up writing this book on top of the training course. This book shines a light on the requirements embedded in the NIS2 Directive. In it, I have tried to stay away from technical approaches, and where the approaches are inevitable (e.g. because the Directive explicitly refers to a technical measure) I have brought the topic back to basic terms that are hopefully comprehensible by anyone sitting in a management body, board of directors, or similar top management function. In writing the book I have discussed topics with a lot of different people in different areas of expertise, ranging from lawyers, CISOs, CIOs, and CEOs, to security engineers, business continuity professionals, and IT experts. Each of them has knowingly or unknowingly helped me put the wording of this book together.

Two people have gone through every single page of the book and provided detailed commentary, namely Ulf Feger and Ite van Aardenne.

Ulf Feger, Group CISO of Arlanxeo Deutschland, and I have been professionally related since mid-2018. I reached out to him because I value his knowledge of information security. His focus on both IT and OT environments across multiple countries in Europe has provided invaluable insights. Ulf has spent hours of his precious time going through the book, providing detailed feedback throughout his review. It is more than fair to say that Ulf's insights and ideas have not only improved the quality of the book, but also enhanced my knowledge of the field. His contributions have been invaluable to me.

Ite van Aardenne, CISO of Intergamma, and, more importantly, a close friend, has provided indispensable advice on every aspect of the book. She was the first person I entrusted with the content, and not without good reason. She is open, critical, fair, and above all extremely knowledgeable in the field of information security. If you like what you are reading in the coming pages, please remember that this book would be less than half its worth without her unrelenting feedback. She has my eternal gratitude and friendship.

This book was somewhat of a surprise to me. I set out to write a training course and ended up with both a training course and a book. Writing a book takes a lot of time, and time is one of the most precious commodities of all. Time that I could (and arguably should) have spent with my family ended up being spent behind my laptop. Never in that entire period have either my wife or my daughters told me to stop, slow down, take it easy, drop the book, spend more time with them, or any other argument that would have made me come to my senses. I am so grateful for their understanding and support. It has allowed me to put together a book that I hope will make a difference to many people out there.

The book is an independent work. You will benefit from the contents of this book without following the training. The training does guide you through the book at a higher level. The book provides more details and practical considerations. Both the book and the courseware include a GAP assessment tool. The version in the book is more detailed than the one in the courseware, making the book suitable for an even wider audience.

I hope you enjoy the book and that it will bring you the benefit I intended it to have when I wrote it. Join me or other trainers for the training that will guide you through the content.

On a final note, I want to thank the anonymous Indian for bringing us the zero. In tribute to their impact on the world we live in, I have decided to start the chapter numbering of this book at 0.

Enjoy the read.

Michiel Benda, August 2024

Endorsements

"What makes this book unique is that it's written by an information security expert who is also knowledgeable in laws and regulations and who has a well-trained eye for detail. Consequently, this book is not a legal interpretation of the NIS2 but contains analyses from an information security perspective with a strong focus on the business needs of the organization. This book provides practical guidance on what organizations must implement, including comprehensible background information that gives the needed context to the NIS2 and its requirements. The Gap Analyses that can be found in one of the annexes proves to be the cherry on top. It provides organizations with a clear overview of where you are and what you still need to do to become NIS2 compliant."
Ite van Aardenne, CISO at Intergamma

"The book provides a comprehensive overview of the current status of the NIS2 Directive and the challenges that all companies and institutions must face in this context to achieve a basic level of cybersecurity maturity and resilience. Therefore, the development, scope, and concepts of the directive in the European context and its requirements are outlined.
The included appendices, e.g. the mapping of the NIS2 to ISO and the tabular GAP assessment for evaluating your own cyber security program, offer great added value.
NIS2 keeps you busy and you need guidance?
This book helped me as it provides a comprehensive overview of the current status of the NIS2 Directive and addresses the challenges all companies and institutions must face in this context to achieve a basic level of cybersecurity maturity and resilience. By reading this book you understand the development, scope, and concepts of the Directive in the European context.
Furthermore, the included appendices, e.g. the mapping of the NIS2 to ISO and the tabular GAP assessment will help you for assessing and evaluating your own cyber security program.
Have in mind this is not meant for one country only and it will be interesting how the Directive will mature in future - maybe towards an EU Regulation. It will also become challenging for companies spread across multiple European countries with their potentially different legal implementations. So, I see this as a start of a longer journey – for mature and not so mature entities."
Ulf Feger, Group CISO at Arlanxeo

"It can't be made easier, but it can be made clearer! Michiel Benda knows how to translate difficult to read directives into easy-to-read texts. The NIS2 Navigator's Handbook offers a very structured and clear explanation of the NIS2. This includes not only what the NIS2 describes and how to implement it meaningfully, but also why the NIS2 was created and which parties played a role in it. The NIS2 Navigator's Handbook - Bridging the cybersecurity GAP will help anyone who wants or needs to delve deeper into NIS2."
Paul Gooijen, CISO at Mosadex Group

"The NIS2 directive is still being translated into legislation, and information is both scattered across various sources and requires interpretation. When reading articles about NIS2, often written by suppliers, these interpretations can vary significantly. Gathering and analyzing all this information to create an authoritative source of knowledge on NIS2 is quite a task. I'm very thankful to be able to reuse Michiel's work in my daily activities as a security professional. Whether it's to gain a better understanding, find an answer to a question, or get help in deciding how to approach NIS compliance within the company, this book is invaluable. I highly recommend it to anyone looking to implement NIS compliance, both within their own company or at a customer's company. Additionally, people already receiving help in the form of consultancy can use the book to verify and control what's happening."
Joran Leenders, CISO at Ypto

0 Purpose

…essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.
- NIS2, Article 21, paragraph 1

…management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.
- NIS2, Article 20, paragraph 1

As an entity falling under the NIS2 scope, your organization is required to have cybersecurity risk measures in place that are appropriate to the risks it faces. A base control set of mandatory controls is specified in NIS2. As management of such an entity, you must be in control of the cybersecurity risks, and you may be held liable for the cybersecurity resilience choices made in the organization. With a personal liability attached to compliance, regardless of how likely it is that you will be held liable, you will want to be able to keep control over the cybersecurity risks and the state of compliance of your organization. Your level of cybersecurity knowledge and skills may lead you to decide to rely on the experts in your team to provide you with sufficient insight.

This book is written for all members of management bodies, including the information security officer and data protection officer. The book describes the requirements in basic terms that are understandable for anyone, without going into the technical details of some of the requirements. Moreover, the book provides an extensive GAP assessment tool that will help you keep track of your compliance status in relation to the NIS2 requirements. The book can be read from cover to cover but is structured in a way that allows it to be used as an easy reference guide as well.

0.1 SOME CLARIFYING NOTES

For readability purposes, this book will refer to Directive 2022/2555 as "NIS2" or the "Directive".

The book often refers directly to "you", what "you" should do, or what something means for "you". "You" in those cases refers to you as the representative of your organization rather than you as an individual. An organization is any legal entity that must abide by NIS2 requirements. It can be a governmental body, national institute, corporation, foundation, self-employed contractor, privately owned company, or any other entity that may need to apply the rules laid down in this Directive.

0.2 DISCLAIMER

This book provides clarification on the NIS2 content. It also helps you assess your organization in relation to the NIS2 requirements and provides you with an understanding of how to achieve compliance. Should you need a formal legal interpretation, you should consult a legal expert on how to interpret the Directive.

0.3 STRUCTURE OF THE BOOK

The book is structured in a logical sequential approach. Beyond the first chapter that contains an overall introduction, chapter 2 will help you understand the purpose of the Directive by leading you through the NIS2 background and origin. This background will help you put NIS2 in the larger context of the European initiatives and strategies aimed at making the EU more digitally resilient and self-supporting. The chapter will also give you some high-level information on the Directive and some idea of the main changes from the first version of the NIS. There have been significant updates since this first version, including the broadening of the scope of the companies that must comply with the Directive.

Chapter 3 takes a deeper dive into the Directive. Beyond an initial implementation timeline, some of the cybersecurity terminology that is used will be explained to you. This is followed by a section in which you will be introduced to a wide range of EU institutions and governmental bodies that play a role in the execution of the NIS2 Directive. Subsequent sections describe the expectation of a National Cybersecurity Strategy and the concept of certification schemes. Section 3.7 distinguishes the types of entities that fall within the NIS2 scope and helps you in classifying where (and whether) your organization falls within this scope. The final two sections of the chapter will explain the requirements that the entities must comply with, as described in NIS2

Chapter IV, and the requirements described in Directive articles 21 and 23 which focus on specific measures you must implement and your reporting obligations.

The contents of the chapter above may lead the reader to wonder what responsibilities the different roles in the organization have. To clarify this, section 3.10 describes the responsibilities for some of the key roles, including management, general employees and third parties.

Chapter 4 of this book helps you determine your own compliance with NIS2. As each requirement is explained, the book emphasizes the questions to ask and statements to verify that will help you determine the gap between your current state and NIS2 compliance.

Table of Contents