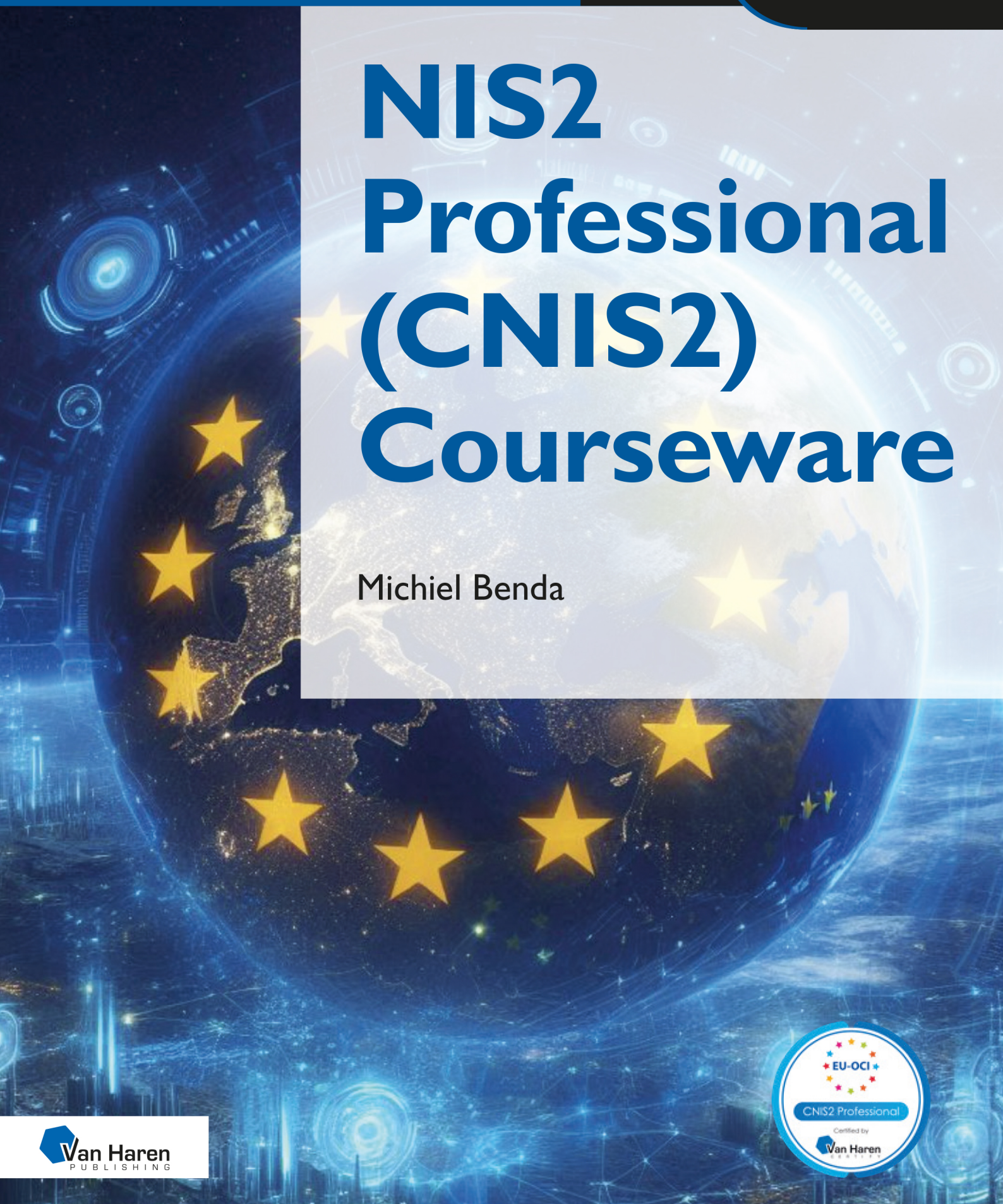
COURSEWARE

NIS2 Professional (CNIS2) Courseware

Michiel Benda



Van Haren PUBLISHING

Certified NIS2 Professional

Courseware v1.0

Colophon

Title:	NIS2 Professional (CNIS2) Courseware
Authors:	Michiel Benda
Publisher:	Van Haren Publishing, ‘s-Hertogenbosch
ISBN Hard Copy:	978 94 018 1188 0
Edition:	First edition, first print, July, 2024
Design:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2024

For further information about Van Haren Publishing please e-mail us at: info@vanharen.net or visit our website: www.vanharen.net

Publisher about the Courseware

The Courseware was created by experts from the industry who served as the author(s) for this publication. The input for the material is based on existing publications and the experience and expertise of the author(s). The material has been revised by trainers who also have experience working with the material. Close attention was also paid to the key learning points to ensure what needs to be mastered.

The objective of the courseware is to provide maximum support to the trainer and to the student, during his or her training. The material has a modular structure and according to the author(s) has the highest success rate should the student opt for examination. The Courseware is also accredited for this reason, wherever applicable.

In order to satisfy the requirements for accreditation the material must meet certain quality standards. The structure, the use of certain terms, diagrams and references are all part of this accreditation. Additionally, the material must be made available to each student in order to obtain full accreditation. To optimally support the trainer and the participant of the training assignments, practice exams and results are provided with the material.

Direct reference to advised literature is also regularly covered in the sheets so that students can find additional information concerning a particular topic. The decision to leave out notes pages from the Courseware was to encourage students to take notes throughout the material.

Although the courseware is complete, the possibility that the trainer deviates from the structure of the sheets or chooses to not refer to all the sheets or commands does exist. The student always has the possibility to cover these topics and go through them on their own time. It is recommended to follow the structure of the courseware and publications for maximum exam preparation.

The courseware and the recommended literature are the perfect combination to learn and understand the theory.

-- Van Haren Publishing

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: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, 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®
CATS CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur
Methode
TOGAF®

Business Management

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

Project Management

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

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

Foreword

When the Network and Information Systems Directive (NIS2) was published in December 2022 it was clear that this Directive was going to make a big impression in Europe. For many companies it was a trigger:

A. To realize that they are going to have to step up their information security game,

B. To prepare a new line of business to help organizations become compliant to the Directive, and

C. To start informing people and organizations alike on the contents of the NIS2 and what it would mean to them.

Point C above has resulted in a vast range of trainings, webinars, seminars, roundtables and more. This courseware distinguishes itself from the others through a combination of several factors:

1. It explains the requirements listed in the Directive by tracing the meaning and intent of them through numerous recitals in the Directive and references to other legal EU publications. For example, rather than just stating that you need to implement human resource security as specified in article 21(2i), this training explains what the NIS2 means for this requirement by tracing the specifications back to recital 79 and EU Directive 2022/2557.

2. It explains the requirements of the NIS2 in simple business terms. Technical terminology is avoided unless the Directive explicitly refers to the terminology itself. In such cases, the terminology will be explained in terms that are as far away from technology as is reasonably possible. This training is meant for those who play a role in governing information security and the compliance to the Directive. That does not require extensive technical knowhow.

3. It provides you with the means to assess your own organization against the requirements of the NIS2. As you go through the requirements, you will be marking your (estimated) state of compliance on the GAP assessment form. At the end of the course, you will have a high-level impression of your state of compliance, along with an overall organizational score. The GAP assessment will also provide you with a clear set of actions that you can take to become fully compliant.

4. It combines this courseware with a two-day course that is provided by certified trainers that have a thorough understanding of information security and the NIS2 Directive. The course allows you to then take an exam to obtain the coveted CNIS2 certification that will evidence your understanding of the requirements of the Directive and your preparedness to support the organization in attaining compliance.

5. It provides you the insights into the Directive from a European perspective, rather than a US perspective. The entire training and the exam are written and reviewed by European natives with expertise in the field of information security. The CNIS2 certification is issued and controlled through a wholly owned European accreditation organization.

About the author

Michiel Benda is a seasoned professional with over 30 years of experience in privacy, IT, and information security. His journey began in hospitality management from where he quickly moved into process automation and IT services. In IT services, Michiel quickly moved through the ranks of IT engineering and management to IT Director for a large multinational company.

Recognizing the increased criticality of information protection, Michiel shifted his career focus to information security. He designed and implemented robust security measures for companies worldwide, ranging from small businesses to large enterprises with thousands of employees, though never compromising on business priorities and operability.

In 2017, driven by a desire to help more organizations, Michiel founded Omni-U through which he provides consultancy, CISO coaching, training and certification guidance. His vision is to enable any organization, regardless of size or information security knowledge and expertise, to protect its business operations and objectives against information security and cyber threats. Michiel is an expert in information security governance and risk management.

The CNIS2 Professional training and courseware reflects Michiel's commitment to the Omni-U vision. Drawing from his extensive knowledge, the training provides practical insights, strategies, and guidance for navigating the complexities of the NIS2 Directive. Whether you're an industry professional, policymaker, or cybersecurity enthusiast, Michiel's expertise will illuminate the path toward a safer digital landscape.

Michiel lives in the serene, forested area of the Veluwe in the Netherlands, where he balances his commitment to a better and safer world with a personal life with a loving family, friends and a love for capturing the world through the lens of his camera.

Michiel Benda: Founder of Omni-U and 0-Effort Solutions, Information Security Expert, and Author.

Disclaimer

The information contained in this manual contains an explanation of the NIS2 Directive and its expectations. You should not be acting on, implementing, or executing any ideas, suggestions, or concepts gained in this manual or the course without due consideration and evaluation of the unique circumstances of the organization in which you wish to apply them.

Both the course and this manual are intended solely to help you assess your organization in relation to the requirements of the Directive and to provide you with an understanding of how to achieve compliance. Neither the course nor the training is meant to serve you as a legal interpretation of the Directive. Any doubts that you have about such interpretations should be addressed by either an internal or external legal expert.

Clarifying notes

For readability purposes, this manual will refer to Directive 2022/2555 as “NIS2” or simply “Directive”.

The manual 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 the individual. An organization is any legal entity that must abide by the 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.

Purpose

> *…the members of the management bodies of essential and important entities are required to follow training…in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.*
>
> *NIS2, Article 20, paragraph 2*

As management of organizations that fall under the scope of the NIS2 Directive, you are required to follow training that is sufficient for you to make informed decisions about your organization's cybersecurity practices. This training is designed to meet that requirement.

As management your time is precious. While training is important, what you probably really want to know is whether you are compliant with the Directive's requirements. This training is designed to meet both needs.

This manual supports the CNIS2 certification course. Both the training and the manual aim to help you prepare for compliance with the NIS2 Directive.

The NIS2 Directive is an instruction to EU Member States to create a national law. Directives include much of what the final national laws will contain but leave room for local/national interpretation. To comply with the national laws that will be drafted, you may need to comply with additional requirements included by each individual Member State in their NIS2 derived legislation.

This manual focuses on the practical implications of the Directive and what the organizations that must comply with it have to do to meet the Directive's intent. It is written for members of management bodies, including the information security officer and data protection officer to provide practical guidance to the requirements in the Directive. The manual will help you assess and prepare for basic compliance with the Directive in a structured and easily comprehensible manner.

The training associated with this manual is further supported by the book "The NIS2 Navigator's Handbook: Bridging the cybersecurity GAP". The book expands on many of the topics in the training to give those that will actively pursue NIS2 compliance a further insight into the law and its interpretation. The book also includes a more detailed gap analysis for an even clearer understanding of what needs to be done in your organization for you to become compliant.

Table of Contents

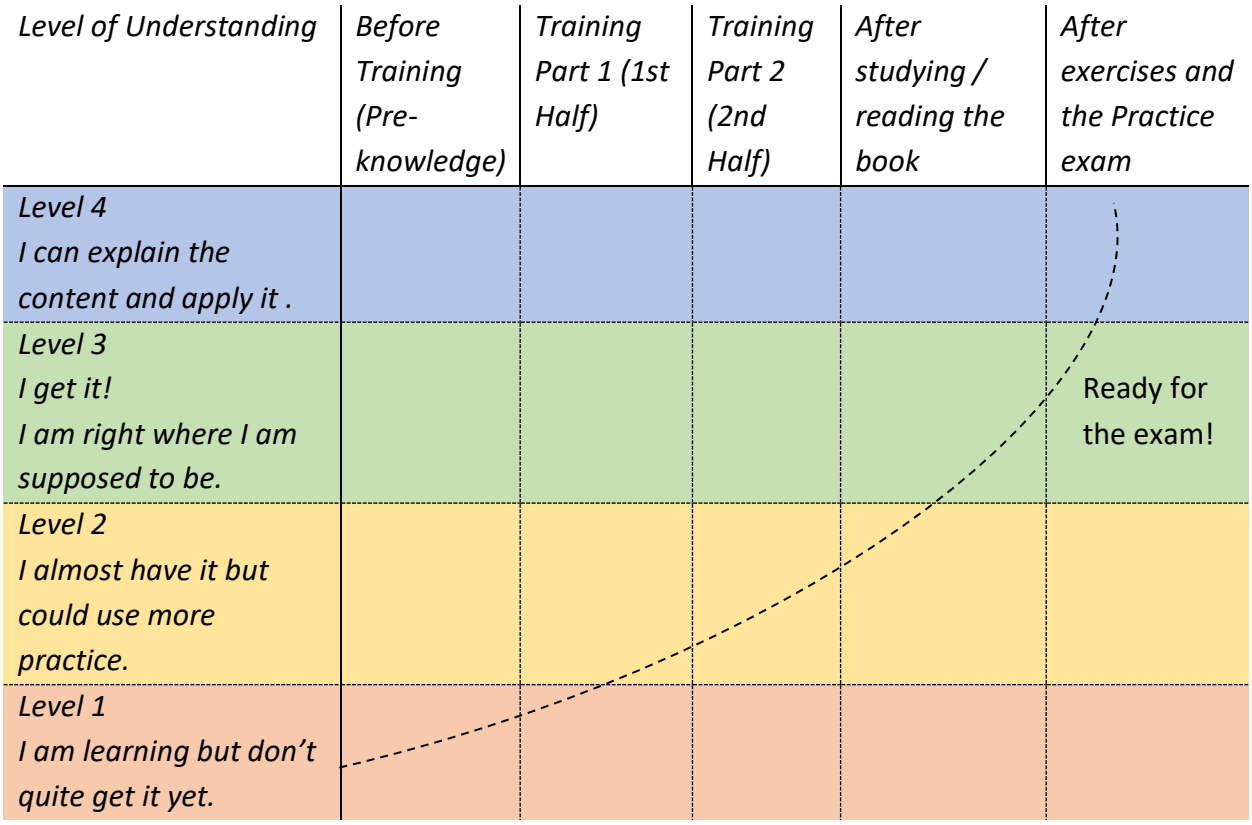
Slide deck

Self-Reflection of understanding Diagram

‘*What you do not measure, you cannot control*.’’ – Tom Peters

Fill in this diagram to self-evaluate your understanding of the material. This is an evaluation of how well you know the material and how well you understand it. In order to pass the exam successfully you should be aiming to reach the higher end of Level 3. If you really want to become a pro, then you should be aiming for Level 4. Your overall level of understanding will naturally follow the learning curve. So, it’s important to keep track of where you are at each point of the training and address any areas of difficulty.

Based on where you are within the Self-Reflection of Understanding diagram you can evaluate the progress of your own training.



(Self-Reflection of Understanding Diagram)

Write down the problem areas that you are still having difficulty with so that you can consolidate them yourself, or with your trainer. After you have had a look at these, then you should evaluate to see if you now have a better understanding of where you actually are on the learning curve.

Troubleshooting

Problem areas:	*Topic:*
Part 1	
Part 2	
You have gone through the book and studied.	
You have answered the questions and done the practice exam.	

Timetable

Day 1: NIS2 Basics

- EU programs background
- NIS2 outline
- Security concepts
- Public bodies and institutes
- Obligations
- Supervision and enforcement
- Roles and responsibilities

Day 2: GAP assessment

- GAP assessment explanation
- Cybersecurity program
- Cybersecurity training
- Risk management
- Policies
- Resilience planning
- Organizational controls
- Technical controls

Syllabus

Certified NIS2 Professional (CNIS2)

Version 1.0

This material contains diagrams and text information based upon:

The NIS2 Navigator's Handbook: Bridging the Cybersecurity Gap ©Van Haren Publishing

About Certified NIS2 Professional (CNIS2)

As cyber risk concerns are becoming increasingly prominent in the risk profiles of organizations, members of senior management bodies are required to understand these risks and make informed decisions for the organization that consider these risks and their impact, not just on the organization itself, but also on the ultimate recipients of their products and services.

IP owner:	EU Organisational Compliance Institute
Accreditation institute:	Van Haren Certify
Examination institute:	certN

The Network and Information Systems Directive released in 2022 (NIS2 Directive) emphasizes the importance of this understanding and involvement by these members of the organization's management bodies by requiring them to actively involve themselves in cybersecurity risk management and the implementation of measures to make these risks justifiably acceptable.

Navigating NIS2: Bridging the Cybersecurity GAP takes you on tour through the NIS2 Directive. It is a tour for these members of the organization's management bodies, whether they are the Chief Information Security Officers, Chief Risk Officers, Chief Executive Officers, or any other member of the management team. This course is unique because it understands that, especially for these members, time is a precious commodity. Hence, this course walks you through the overall Directive in the first day and takes you through a NIS2 assessment of your own organization on the second day. As attendee, you will not only complete the tour with an understanding of what the NIS2 means, but specifically what it means to you and what you should do to become compliant.

Certification definition

The CNIS2 certification validates a candidate's understanding of the Directive including the measures that it prescribes. The certification also verifies the candidate's knowledge about basic information security concepts that enable the candidate to discuss the cybersecurity risk management measures with those that are charged to implement and maintain them.

Certification definition

Candidates can become certified by passing the Certified NIS2 Professional exam.

Vouchers for the certification exam are available through accredited trainers and Van Haren Group.

Certification renewal

The CNIS2 Professional certificate is valid indefinitely.

The certificate you receive after passing the exam shows the date of issue. It also indicates how long the certificate is valid.

Exam format

The general exam regulations apply to this exam.

Attemps per voucher:	1
Number of questions:	40
Passing score:	60%
Passing score for trainers:	75%
Time:	60 min.
Open book:	No
Language:	Engels
Invigilation:	Yes
Question type:	multiple choice

Exam syllabus

The following table is an overview of the topics examined in the certification exam.

Module	Exam Requirements	Exam Specification	Bloom level	Weight %	Book	Courseware
1	Background			10%		
1.1		Cybersecurity in the Union	1		Ch 2.1-2.4	Ch 1.1
1.2		EU cybersecurity strategies and programs			Ch 2.2	Ch 1.2-1.5
1.3		EU Regulatory Framework			Ch 2.4.2	Ch 1.6
2	Directive structure			15%		
2.1		NIS Directive	1		Ch 2.2.3, 2.5	Ch 2.1
2.2		NIS2 Scoping	1		Ch 3.6-3.7	Ch 2.2-2.3
2.3		NIS2 Structure			Ch 3.1, 3.3	Ch 2.4
2.4		NIS2 bodies and institutions			Ch 3.5	Ch 4
3	Entity roles, responsibilities, and obligations			15%		
3.1		Roles and responsibilities	1 + 2		Ch 3.10	Ch 6
3.2		Entity requirements	1		Ch 3.8	Ch 5.1-5.4
3.3		Supervision and enforcement			Ch 3.9	Ch 5.5
4	Security concepts			10%		
4.1		Basic security concepts	2		Ch 3.4	Ch 3
5	Cybersecurity risk-management measures			30%		
5.1		Cybersecurity program	1		Ch 4.1	Ch 7.1
5.2		Risk management	1		Ch 4.3	Ch 7.2
6	Implementation			20%		
6.1		Implementing measures			Ch 4.2, 4.4-4.8	Ch 7.3-7.15
6.2		Reporting to the management body			Ch 3.8.2, 3.10.1, 3.10.2	

* More information about the levels of cognition click here

Reference Material

The reference material for the Certified NIS2 Professional exam is:

- The NIS2 Navigator's Handbook: Bridging the Cybersecurity Gap
- Author: Michiel Benda
- Publisher: Van Haren Publishing

Trainer accreditation

Van Haren Learning Solutions organizes the trainer accreditation for this certification program. More information on the accreditation process can be found on their website.

1 Background

On 27 December 2022, the European Union published four new directives and regulations. These four publications are closely related to each other as each of them addresses organizational resilience for European entities that are critical to the functioning of the economy of the European Union and its society. The publications are listed below.

- **DORA (2022/2554)**
  DORA stands for Digital Operational Resilience Act. It is a regulation introduced for the financial sector. It is focused on resilience from a broad ICT perspective. Entities that must follow DORA are likely to have to follow NIS2 as well.
- **Amendments based on DORA (2022/2556)**
  This directive provides updates to other, existing directives to align them with the DORA regulation. By changing these directives, the EU is instructing Member States to update the legislations they drafted based on the mentioned directives.
- **NIS2 Directive (2022/2555)**
  NIS2 Directive stands for Network and Information Systems Directive version 2. It is a directive focused on the cyber resilience of entities in the European Union that EU citizens are most reliant on for their safety, security, and welfare. It succeeds the NIS Directive of 2016.
- **CER Directive (2022/2557)**
  CER Directive stands for Critical Entities Resilience Directive. It addresses the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental, or intentional. It addresses an organization's resilience beyond cybersecurity resilience and extends to physical threats such as terrorist offences, sabotage, and natural disasters. Entities identified as critical under the CER are considered essential under the NIS2. The requirements specified in the NIS2 supersede any conflicting requirements in the CER.

Of the four publications, three address resilience in the digital operations of the organization. Cybersecurity is at the forefront of each of them.

1.1 Cybersecurity in the European Union

Digital technologies are essential to most EU citizens and businesses. Disruptions could have a significant effect on the EU's role in world society. The Union's dependency on systems and solutions coming from other regions of the world creates a further concern that the EU is ill-equipped to control such disruptions. Malicious cyber activities may threaten its economy as well as its citizens directly. On some instances, these malicious activities may even try to undermine the cohesion and functioning of the democracy in Europe.

Cybersecurity has been on the EU agenda since the beginning of the century. It is considered fundamental to the resilience, security, and trustworthiness of Europe's digital infrastructure, services, and economy.

Cybersecurity is crucial to the future of the EU for several reasons:

- **Critical Infrastructure must be protected.**
  Critical infrastructure, such as energy, transportation, healthcare, and financial systems, rely on

digital technologies. Their continuous operations are essential to the welfare of EU citizens and the economy as well as to sustain the functioning of society.

- **Economic Competitiveness must be maintained.**
  A secure and trustworthy digital environment is essential to maintain global economic competitiveness. Good cybersecurity provides trust and confidence in digital services, which in turn will fuel innovation, provide economic growth, and maintain competitiveness.
- **Personal Data and Privacy must be protected.**
  Privacy is high on the EU agenda. Personal data must be protected in the digital environment using robust cybersecurity measures to sustain the rights and freedoms of EU citizens.
- **The EU economy must be defended against cyberthreats.**
  Cybersecurity is a critical part of EU defenses against cyberthreats such as cybercrime, state-sponsored attacks, and cyber-espionage. As these threats evolve, the EU cyber-defense mechanisms must evolve with them to protect national security and maintain the integrity of EU institutions and processes.
- **EU citizens should be able to trust digital services and be empowered in their use.**
  Everyone should be able to trust digital technologies and feel empowered in their digital interactions. Cybersecurity measures protect individuals from cyber risks, fraud, and online abuses, and allow them to fully participate in the digital society.

1.2 The Cybersecurity Strategy of 2013

In 2013 the EU adopted a cybersecurity strategy that focused on building a secure and trustworthy digital environment within the European Union. The strategy outlined five priorities.

1. **Make network and information systems cyber resilient.**
   The strategy achieves resilience by:
   - Promoting risk management practices,
   - Establishing and emergency response team for European Union's institutions, bodies, and agencies (the CERT-EU), and
   - Engaging in partnerships between public and private institutions.
2. **Reduce cybercrime.**
   Reduction of cybercrime is approached through legal frameworks and laws, including enforcement capabilities.
3. **Define a European cyber defense policy framework.**
   Establishing a European cyber defense policy framework involves:
   - Improving cooperation and information-sharing among Member States,
   - Conducting cyber defense exercises, and
   - Supporting research and development in the field of cybersecurity.
4. **Enhance EU cybersecurity technologies.**
   Enhancing industrial and technological resources for cybersecurity is accomplished by:
   - Encouraging research and innovation,
   - Promoting the development of cybersecurity standards, and
   - Supporting the certification of products and services.

5. **Creating and maintaining international cyberspace cooperations**.
   The cooperations should be aimed at facilitating an open, secure, and stable cyberspace. The cooperations could be between Member States and countries as well as between public bodies and international partners. These cooperations would contribute to the development of and publish international norms and standards for cybersecurity.

The GDPR is one of many accomplishments of the strategy.

1.3 The Cybersecurity Strategy for the Digital Decade

The European Commission decided to make the 20's Europe's "Digital Decade". In it, Europe must strengthen its digital sovereignty and set standards, rather than following those of other sovereignties such as the USA – with a clear focus on data, technology, and infrastructure.

In December 2020, the European Commission presented the EU's Cybersecurity Strategy for the Digital Decade as a revision of the Cybersecurity Strategy of 2013. The Cybersecurity Strategy for the Digital Decade aims to:

- Develop the EU's technological sovereignty in cybersecurity,
- Build capacity to secure sensitive infrastructures such as 5G networks,
- Reduce dependence on other parts of the globe for crucial technologies,
- Bolster Europe's resilience against cyber threats, and
- Promote trust in the digital economy.

To ensure the successful execution of the strategy, policies and investments in the Union's cybersecurity are indispensable.

The Cybersecurity Strategy for the Digital Decade has three main objectives:

1. To strengthen the EU's collective resilience against cyber threats,
2. To promote a global and open cyberspace, and
3. To advance a coherent EU cyber diplomacy.

It outlines several key actions to achieve its objectives, including:

- Developing a body that will strengthen the EU's response to large-scale cyber incidents,
- Strengthen cybersecurity of critical sectors, such as energy, transport, and finance,
- Enhancing the legal framework for cybersecurity, including a replacement of the NIS Directive, and
- Establishing a global framework for responsible state behavior in cyberspace.

1.4 Europe Fit for the Digital Age

The "Europe Fit for the Digital Age" program was launched by the European Commission in December 2019. The program can be seen as a strategic framework through which the EU recognizes the significance of digital transformation and the need to adapt and prepare Europe and its population for the opportunities and challenges presented by the digital age.

The framework encompasses various initiatives, policies, and objectives aimed at preparing Europe for the digital transformation and harnessing the potential of digital technologies for the benefit of the EU citizens and economy.

The program focuses on the below key priorities:

- **Digital Skills**: Promoting digital literacy and ensuring that Europeans have the necessary skills to thrive in the digital era,
- **Digital Infrastructure**: Expanding high-speed connectivity, including 5/6G networks and widespread access to broadband, to ensure reliable and fast digital services,
- **Digital Economy and Society**: Supporting the growth of the digital economy, fostering innovation, and creating a favorable and secure environment for businesses to embrace digital technologies, and
- **Digital Governance**: Establishing clear rules and frameworks to address emerging digital challenges, including data protection, cybersecurity, and ethical use of artificial intelligence.

1.5 The Digital Europe Program

The Digital Europe Program (DIGITAL) is a funding program of €7.5 billion that aims to address the target of a climate-neutral Europe by bringing digital technology to businesses, EU-citizens, and public administrations alike, but particularly to small and medium-sized enterprises.

It supports projects in five key capacity areas:

1. Supercomputing,
2. Artificial intelligence,
3. Cybersecurity and Trust,
4. Advanced digital skills, and
5. Digital Innovation Hubs.

DIGITAL provides financial support for cybersecurity measures and technology upgrades that are required for NIS2 compliance.

1.6 The EU regulatory framework

The Europe Fit For The Digital Age Program, the Digital Europe Program, and the EU Cyber Security Strategy all require a regulatory framework to enhance resilience and strengthen the EU's capability to operate independently of other nations. The framework consists of several directives and legislations.

1.6.1 The Digital Markets Act (2022)

The Act fosters fairer digital markets. It identifies large digital platforms, such as search engines, app stores, and messenger services, as "gatekeepers". These gatekeepers are subject to specific requirements, such as access and interoperability to ensure fair competition, prohibition of self-preferring, transparency and fair ranking by disclosing the ranking algorithms, and the prohibition of practices that harm competition.

1.6.2 The Digital Services Act (2022)

The Act regulates online intermediaries and platforms, such as marketplaces, social networks, content-sharing platforms, app stores, and online travel platforms. It aims to prevent illegal and harmful activities online, reduce the spread of disinformation, and create a fair and open online environment.

1.6.3 The Network and Information Systems Directive (2023)

Defining measures for a high common level of cybersecurity across the Union. The revised version (NIS2) entered into force on January 16th, 2023.

1.6.4 The Critical Entities Resilience Directive (2023)

The Directive enhances the resilience of entities which provide services vital for societal functions and economic activities. The Directive ensures that these entities can prevent, withstand, absorb, and recover from disruptions, such as natural hazards, terrorism, insider threats, sabotage, and health emergencies.

1.6.5 The Digital Operational Resilience Act (2023)

The Act strengthens IT security for financial entities like banks, insurers, and investment firms. It harmonizes rules across 20 types of financial entities and ICT third-party service providers, ensuring their resilience during severe operational disruptions.

1.6.6 The European Digital Identity Wallet (2023)

The EU Digital Identity Wallet allows citizens to prove their identity across the EU when accessing online services, sharing digital documents, or verifying specific personal attributes (such as age) without revealing full identity details. It enhances security and convenience for both users and businesses.

1.6.7 The European Chips Act (2023)

The Act aims to strengthen Europe's technological leadership in semiconductor technologies and applications. It addresses global semiconductor shortages and supply chain challenges by supporting large-scale production, innovation, research, and skills in the chip industry.

1.6.8 The Artificial Intelligence Act (2024)

The Act aims to establish harmonized rules for artificial intelligence (AI) within the European Union. It addresses both the benefits and risks associated with AI, ensuring that its development aligns with EU values, fundamental rights, and principles. The act covers definitions, risk classification, prohibitions, rights protection, governance, and enforcement.

1.6.9 The European Data Act (2024)

The Act was designed to enhance the EU's data economy and promote a competitive data market. The Act makes data (e.g. industrial data) more accessible and usable, encouraging data-driven innovation and increasing data availability. One of the ways in which the Act aims to accomplish this is by clarifying who can create value from data and under which conditions. In this way, it contributes to advancing digital transformation and establishing an EU single market for data. It encourages secure data sharing across sectors, benefiting both the European economy and society at large.

1.6.10 The Cyber Resilience Act (2024)

The Act aims to enhance cybersecurity for products and software with digital components. It mandates cybersecurity requirements for manufacturers and retailers, ensuring safer products throughout their lifecycle. Consumers and businesses benefit from improved security and informed choices when purchasing CE-marked products.

NIS2 Directive basics

2 Network and Information Systems

2.1 The NIS Directive of 2016

In 2016, the Network and Information Systems (NIS) entered into force. It most Member States, the Directive was adopted into local legislation in 2018.

The intention of the NIS was to set up uniform cybersecurity capabilities across the Union. Its scope was directed at the network and information systems of entities that provided essential services in key sectors. Essential services were seen as the services that, when disrupted, would significantly affect the functioning of the Union's economy and society.

NIS has proved to be very effective as the cyber resilience of the scoped entities, which includes both private and public bodies, has improved significantly. Some of the outcomes of the NIS are:

- The completion of national frameworks and strategies on the security of network and information systems,
- The establishment of national cybersecurity capabilities,
- The implementation of regulatory measures covering essential infrastructures and entities identified by each Member State, and
- Better cooperation between Member States through the establishment of the Cooperation Group and the network of national computer security incident response teams.

Since the adoption of the NIS, there have been significant changes in the world, and, despite the above-mentioned achievements, reviews revealed inherent shortcomings that prevent the NIS from effectively addressing current and emerging cybersecurity challenges. As a result, the Cybersecurity Strategy for the Digital Decade has included the initiative to update the NIS Directive.

2.1.1 Shortcomings of the NIS Directive

Network and information systems play an ever-increasing central role in everyday life. Digital transformations, cross border exchanges and borderless digital social interactions have become more common and expected societal elements. This growth of cyber opportunities brings a growth of cyber threats at the same time. The expansion of the cyber landscape introduces new challenges which require better coordinated and innovative responses.

Since the adoption of the NIS Directive, the number, magnitude, sophistication, frequency, and impact of cyber related incidents has been growing, often exponentially. These cyber threats pose a major concern to the functioning of the Union and the individual Member States. They can impede economic activities, generate financial loss, undermine user confidence, and cause major damage to the functioning of the EU economy and society. An effective cybersecurity program and preparedness of the entities contributing to the functioning of the economy and society have therefore become more essential than ever to the proper functioning of the European internal market. These changes in the landscape are insufficiently addressed in the NIS Directive in several areas, including the scoping of entities, where the impact of the supply chain was underestimated, as well as approaches to address the threats.

The insufficiency is caused in part by the variations in the implementation of the NIS in the various Member States. Great differences exist in both requirements and supervision. In some cases, the interpretations of requirements outright conflict between countries' NIS implementations which burdens companies that offered cross-border services and products disproportionately.

2.1.2 How NIS2 improves on the NIS Directive

The NIS2 Directive is introduced to address the shortcomings of the NIS and to prepare the Union for a more dynamic cyber landscape, with even more reliance on the landscape by most entities operating in the Union. It introduces new requirements to further improve the EU's cyber resilience and to address the significant increase in the use of third-party services and cloud computing environments.

The NIS2 Directive now enhances the original NIS through the following points:

- New requirements are added to address supply chain security,
- More concrete requirements are included to address supervision by Member States, including more diligence in imposing penalties on entities that fail to comply with the Directive,
- The classification of "Operator of essential services" was replaced by two new classifications of "essential" and "important",
- Many new entity types were added to the scope to improve EU security and resilience, amongst which are many of the subcontractors and service providers with access to critical infrastructure.

The enforcement mandate for authorities is extended significantly. A strict reporting requirement is also added in which entities must report any incident within 72 hours, with an early warning within 24 hours. This allows authorities to react quickly and improve the chance to contain the cyber threat and limit its impact on the functioning of the economy and society as much as possible. In the event of a security incident and a refusal to cooperate with the authorities, NIS2 provides Member States with a right of injunction, essential forcing organizations to adhere to the instructions or sidestep management of the organization to enforce the instructions. Depending on the classification of the entity that is in violation of the regulations, authorities may also issue fines of up to 2% of turnover.

2.2 NIS2 scope

The NIS2 applies to both public and private entities. The Directive has a list of sectors and entity types defined in its Annexes I and II which are included in the scope if they are at least medium-sized enterprises as described in figure 2.1.

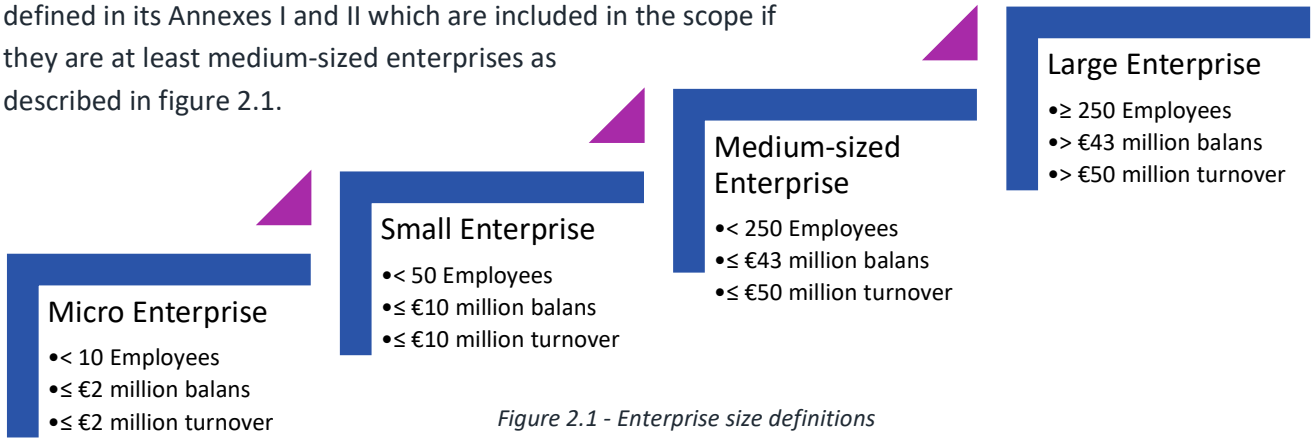


Figure 2.1 - Enterprise size definitions

When calculating the size of the enterprise, the number of employees is calculated based on full-time employment and includes third-party contractors, although it excludes trainees. Anyone working part-time is calculated based on the relative amount of time that they work. There are further considerations based on whether the organization is a partner or linked enterprise. These considerations should be viewed in line with the definitions provided in the Annex to Commission Recommendation 2003/361.

There are some exceptions to the size restrictions. The NIS2 applies to all entities, regardless of their size, that are:

- Providers of public electronic communications networks or of publicly available electronic communications services,
- Trust service providers,
- Top-level domain name registries and domain name system service providers,
- The sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities,
- Providers of services that, when disrupted, could have a significant impact on public safety, public security, or public health,
- Providers of services that, when disrupted, could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact,
- Critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State,
- Public administration entities of central government,
- Public administration entities at regional level that, following a risk-based assessment, provide services the disruption of which could have a significant impact on critical societal or economic activities.
- Designated as Critical Entities under the CER,
- Entities providing domain name registration services.

Member States may choose to have the NIS2 apply to public administration entities at local level and education institutions, in particular where they carry out critical research activities.

Not scoped	Not typed	Essential			Decided by member state	Important	Excluded
				Large Annex I entities	Sole providers of essential societal or economic activity in sector of Annex I or II	Medium-sized Annex I entities	Exclusions from DORA scope
		Trust services from national or public security, defense, or law enforcement	Domain Name Service providers	Top Level domain registries	Entities with significant impact on public safety, security or health in sector of Annex I or II	Large or medium-sized Annex II entities	Entities exclusively servicing national or public security, defense, or law enforcement
	Educational, particularly in critical research	CER nominated entities	Central government	DNS service providers	Entities that can cause systemic risk with potential cross-border impact in sector of Annex I or II	Non-large regional government	Entities carrying out activities in national or public security, defense, or law enforcement

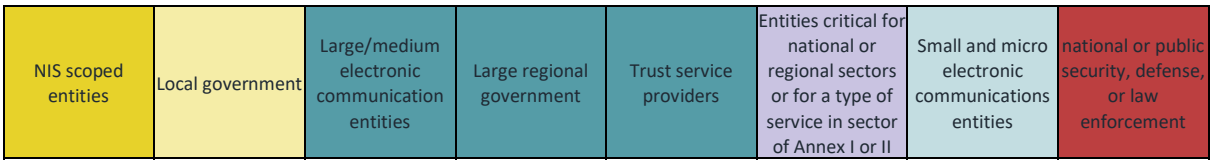


Figure 2.2 - Entities scope and type overview

2.3 Types of entities

Combined, the Critical Entity Resilience Directive (CER) and the NIS2 have introduced three classifications of entities, namely Critical, Essential, and Important Entities.

- **Critical Entities**: This is a type identified in the CER. Critical entities provide services that are crucial for the functioning of the economy, society, public health & safety, or the environment.
- **Essential Entities**: Like Critical Entities, the entities provide services that are crucial for the functioning of the economy, society, public health & safety, or the environment. Such entities are typed as Essential Entities in the NIS2 as providers of crucial services that rely on digital technologies to provide those services.
- **Important Entities**: Entities that provide services in crucial areas but have been excluded from the list of Essential Entities may be marked as Important Entities. Likewise, Important Entities may be providers of services that are critical to the crucial services provided by Essential Entities.

The entities in the scope of the NIS2 are classified as Essential and Important Entities.

NIS2 includes two Annexes that specify the entity types that may be considered essential and important. Further scoping is defined by a set of rules, in which size is the primary factor, excluding most micro and small enterprises. All entities that the CER considers Critical Entities are considered Essential Entities, regardless of whether they are specified in the list of entities in scope in the NIS2 annexes.

NIS2 specifies the classification of many entity types but allows for Member States to expand on the list as needed. Member States are expected to have a list of essential and important entities established by 17 April 2025. A graphical overview of the different entity types in relation to the scope entities can be found in figure 2.2, page 20.

2.3.1 Critical entities

The Critical Entities Resilience Directive addresses resilience of entities that provide critical services in the Union whose disruption can have significant impact on the functioning of the economy and society.

The Directive addresses resilience from a broad spectrum, focusing on everything that is needed for the scoped entities to be resilient against disasters. For cyberthreat based disruptions the CER refers to the NIS2.

Critical Entities is a term that is used in the CER. From a NIS2 perspective, any entity that is identified as critical by the CER must be an essential entity (article 3(1f)) under the NIS2. Critical entities are public or private entities that:

- Provide one or more essential services,
- Operate in the European Union,

- Have their critical infrastructure located in the EU, and
- Could cause a significant disruption if they are affected by an incident.

2.3.2 Essential entities

Essential entities are entities whose disruption will have a significant impact on the EU and its economy, public safety, public security, or public health. The NIS2 has identified a set of rules that determine which entities must be classified as essential. Entities are considered essential when:

- They are listed in Annex I of the directive and are larger than medium-sized enterprises,
- They are qualified trust service providers, top-level domain name registries, or DNS service providers, regardless of size,
- They are at least medium-sized enterprise providing public electronic communications networks or publicly available electronic communications services,
- They are central government public administration entities, excluding entities in the areas of national security, public security, defense, or law enforcement,
- They are regional government public administration entities that provide services that, when disrupted, significantly impact on critical societal or economic activities,
- They are the sole providers in a Member State of a service which is essential for the maintenance of critical societal or economic activities,
- The disruption of their service could have a significant impact on public safety, public security, or public health,
- The disruption of their service could induce a significant systemic risk (the risk of a breakdown of an entire system rather than simply the failure of individual parts), in particular for sectors where such disruption could have a cross-border impact,
- They are critical because of specific importance at national or regional level for the sector or type of service, or for other interdependent sectors in the Member State, or
- They have been identified as critical entities under the CER.

If a Member State expanded the list of operators of essential services prior to the point where the NIS2 entered into force, these operators can be included as essential entities under the NIS2.

2.3.3 Important entities

Entities of a type referred to in Annex I or II, which do not qualify as essential entities are important entities. This includes entities identified by Member States as important entities because:

- The entity is the sole provider of a service which is essential for the maintenance of critical activities,
- Disruptions of the service provided by the entity can have significant impact on public safety, public security, or public health,
- Disruption of the service provided by the entity could result in a cascading of disruptive, possibly even cross border, events (systemic risk), or
- It has specific importance at national or regional level for a particular sector or type of service, or for other interdependent sectors.

2.3.4 Differences between essential and important entities

Recital 15 of the NIS2 states that entities falling within the scope of the NIS2 should be classified into essential entities and important entities. The classification should reflect the extent to which they are critical in relation to the sector in which they operate or the type of service they provide, as well as their size.

The supervisory and enforcement regimes for those two categories of entities are differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other.

The NIS2 has created a must stricter set of requirements for supervision of essential entities than for important entities.

2.4 Structure of the NIS2

2.4.1 Directive versus regulation

NIS2 is a Directive. It should be seen as an instruction to the Member States to create a national law based on the requirements stipulated in the Directive. Directives have different types of requirements. Member States will be required to:

- Embed some of the requirements into the national law without any structural changes in the wording compared to the text of the Directive,
- Interpret the requirements and align them to what fits best in relation to their national laws, and
- Choose to include requirements in the law or leave it out completely.

The NIS2 entered into force on 16 January 2023. Member States were given 21 months to translate the Directive to national law. Hence, by 17 October 2024, Member States must adopt and publish the national law that complies with the NIS 2 Directive. The national law will immediately apply, which means that starting 18 October 2024 at the latest, entities must comply with the national legislation which was derived from the NIS2.

Until a Member State transcribes the Directive into national law, the scoped entities within that Member State are free from any of the obligations of the Directive.

2.4.2 Recitals and provisions

The NIS2 is made up of recitals and provisions. The recitals are the text at the start of the NIS2 that describe the context of the directive and give an idea of how to interpret the provisions. They are introduced by the word “Whereas" and are numbered from 1 to 144.

Recitals in themselves have no legally binding consequences in the same way that the provisions have. Provisions are concise but often leave room for interpretation. If a provision can be interpreted in different ways, the recitals provide context into how the provisions should be read. The Court of Justice of the EU (CJEU) takes a "purposive" interpretation to NIS2. If the text of a provision is unclear, rather than approaching it literally, the CJEU will interpret it to the aim or spirit of the legislation as contextualized in the recitals. However, the content of operative provisions always overrules the content of any associated recitals: if recitals are inconsistent with a provision, then the text of the provision will take precedence.

Provisions state the legally binding requirements. They are divided into chapters, articles, and, where appropriate, paragraphs, each separately numbered. There are nine chapters in the NIS2 and forty-six articles. The articles are uniquely numbered as individual provisions throughout the NIS2. The numbering of the articles is continual and uninfluenced by the chapter divisions.

Many articles are extensive and address the requirements they describe for different situations and types of entities. Where this is the case, articles are divided into paragraphs. Some paragraphs are extensive and may have a further division into subparagraphs. The number of the articles is represented in this manual as follows:

Article 21(2g) = Article 21, Paragraph 2, Subparagraph g

2.4.3 The nine chapters of the NIS2

The NIS2 is divided into nine chapters and three annexes. Each is briefly described below:

- **Chapter I: General provisions**
  A general outline of the NIS2, including a description of the subject matter, the scope, alignment to other laws and the definitions of terms.
- **Chapter II: Coordinated cybersecurity frameworks**
  National requirements for each Member State, including the development of a national cybersecurity strategy and the designation or establishment of various institutions and authorities.
- **Chapter III: Cooperation at Union and international level**
  The requirements at Union level and formalization of the desire to cooperate internationally.
- **Chapter IV: Cybersecurity risk-management measures and reporting obligations**
  The requirements that each entity must comply with.
- **Chapter V: Jurisdiction and registration**
  Jurisdictional clarifications on where entities are represented in multiple Member States.
- **Chapter VI: Information sharing**
  The possibilities to share findings on a voluntary basis.
- **Chapter VII: Supervision and enforcement**
  The rights of authorities and consequences of violation of the NIS2.
- **Chapter VIII: Delegated and implementing acts**
  Delegated acts that may introduce specifications on the law that are legally binding, and the implementing acts that facilitate the implementation of the law into a Member State's legislative framework.
- **Chapter IX: Final provisions**
  Maintenance and implementation of the NIS2.
- **Annex I & II: Sectors, subsectors, and entity types in scope of the NIS2**
- **Annex III: Correlation table to the original NIS**