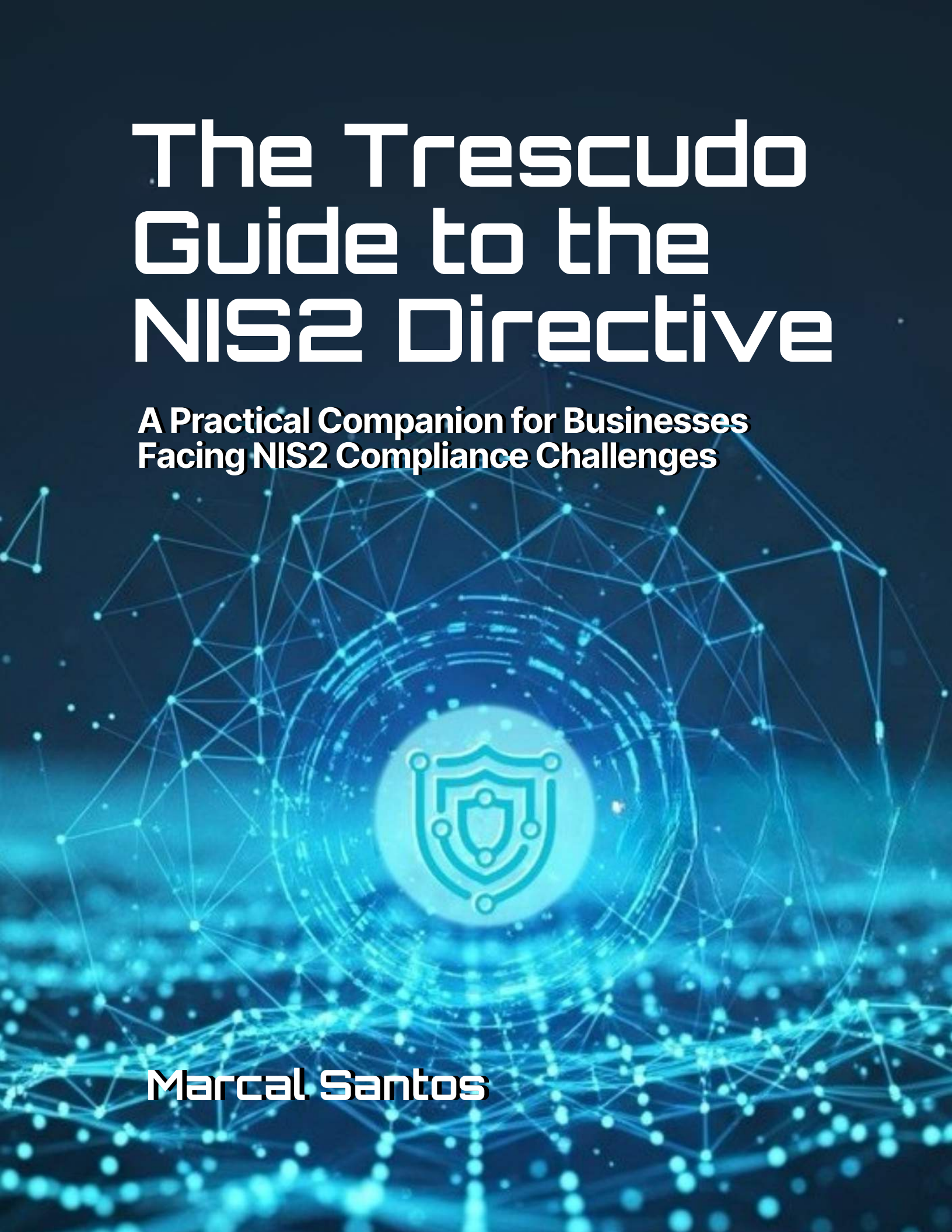
The Trescudo Guide to the NIS2 Directive

A Practical Companion for Businesses Facing NIS2 Compliance Challenges



Marcal Santos

Table Of Contents

A Practical Checklist for Benelux Businesses

Introduction

The EU's Network and Information Systems Directive 2 (NIS2) has now significantly raised the bar for cybersecurity across all critical sectors. The deadline for EU member states to transpose this directive into national law was October 17, 2024. NIS2 is now in effect, imposing stricter security and reporting obligations and moving cybersecurity from a purely technical issue to a core board-level responsibility.

At Trescudo, we help businesses navigate complex regulatory landscapes. This guide is designed to help you understand your obligations under NIS2 and assess your readiness.

a) Does NIS2 Apply to Your Business?

NIS2 applies to a wide range of sectors, categorizing entities as either "Essential" or "Important" based on their criticality and size.

- **Sectors Covered:** The scope includes sectors of high criticality (e.g., Energy, Transport, Banking, Health, Digital Infrastructure, Public Administration) and other critical sectors (e.g., Postal Services, Waste Management, Manufacturing of certain critical products, Digital Providers like social media platforms).
- **Entity Classification:**
  - **Essential Entities:** Generally, these are large organizations (250+ employees or €50M+ turnover) in sectors of high criticality.
  - **Important Entities:** Generally, these are medium-sized organizations (50-249 employees or €10M-€50M turnover) in either high-criticality or other critical sectors.

Even if you are a smaller entity, you may fall within the scope if you are a sole provider in a Member State or have a critical role in a supply chain. A thorough assessment is crucial.

b) Why Compliance Matters:

Understanding the Penalties NIS2 introduces significant penalties for non-compliance, making it a critical business risk. The directive empowers national authorities to impose substantial fines, ensuring management accountability.

- For **Essential Entities**, fines can go up to €10 million or 2% of the total worldwide annual turnover, whichever is higher.
- For **Important Entities**, fines can reach up to €7 million or 1.4% of the total worldwide annual turnover, whichever is higher.

Beyond fines, management can be held personally liable, and non-compliance can lead to reputational damage and loss of customer trust.

The NIS2 Readiness Checklist

Use these questions to identify potential gaps and prioritize your compliance efforts.

1. Governance & Accountability

NIS2 places direct responsibility on management for overseeing and approving cybersecurity risk-management measures.

- [ ] **Management Oversight:** Is cybersecurity a regular agenda item at the board level? Is management actively involved in approving security strategy and measures?
- [ ] **Training for Leadership:** Has the management body received specific training to understand and assess cybersecurity risks and their impact on the business?
- [ ] **Clear Accountability:** Are the roles and responsibilities for cybersecurity risk management clearly defined and assigned within the organization?

2. Risk Management & Security Policies (Article 21)

Entities must take appropriate and proportionate technical, operational, and organizational measures to manage risk.

- [ ] **Risk Analysis Policy:** Do we have a formal policy for conducting risk analysis and ensuring the security of our information systems?
- [ ] **Effectiveness Assessment:** Do we have policies and procedures to regularly assess the effectiveness of our cybersecurity measures (e.g., via audits, penetration testing)?
- [ ] **Cyber Hygiene & Training:** Do we enforce basic cyber hygiene practices (e.g., software updates, password policies) and provide regular cybersecurity training for all employees?
- [ ] **Cryptography & Encryption:** Do we have clear policies regarding the use of cryptography and, where appropriate, encryption to protect data at rest and in transit?

3. Minimum Technical & Operational Measures (The "Duty of Care")

NIS2 mandates a baseline of specific security measures that must be implemented.

- [ ] **Incident Handling:** Do we have an established process for incident handling (detection, analysis, containment, and response)?
- [ ] **Business Continuity:** Do we have a business continuity and disaster recovery plan, including backup management and crisis management protocols, to handle major incidents?
- [ ] **Supply Chain Security:** Do we assess the cybersecurity practices of our direct suppliers and partners? Are security requirements included in our contracts?
- [ ] **Vulnerability Management:** Do we have a process for handling and disclosing vulnerabilities discovered in our systems?
- [ ] **Access Control & Asset Management:** Do we enforce strong access control policies? Do we maintain a comprehensive inventory of our critical assets?
- [ ] **Authentication:** Is Multi-Factor Authentication (MFA) or continuous authentication used for access to critical systems, data, and remote connections?

4. Incident Reporting Obligations

NIS2 enforces a strict, multi-stage process for reporting significant incidents.

- [ ] **Reporting Capability:** Do we have the technical and procedural capability to detect a significant incident and gather the necessary information for reporting?
- [ ] **24-Hour Early Warning:** Do we have a plan to submit an "early warning" to the competent authorities (e.g., national CSIRT) within 24 hours of becoming aware of a significant incident?
- [ ] **72-Hour Incident Notification:** Can we provide a more detailed incident notification within 72 hours, including an initial assessment of its severity and impact?
- [ ] **Final Report:** Do we have a process to compile and submit a final report within one month of the incident?

c) How Trescudo Accelerates Your NIS2 Compliance

This checklist highlights the core pillars of the NIS2 Directive. The time for preparation is over; the era of NIS2 compliance is here.

As your cybersecurity navigator in the Benelux region, Trescudo specializes in translating these legal requirements into a practical and effective security strategy.

Here's how our offerings map directly to key NIS2 requirements:

NIS2 Requirement	How Trescudo's Offerings Help
Governance & Risk Management	Our Cybersecurity Advisory and CISO-as-a-Service offerings help you build the required policies, conduct risk assessments, and establish board-level oversight.
Incident Handling	Our EDR/XDR solutions provide the advanced detection and visibility needed, while our Incident Response services help you build and test your response plan.
Business Continuity & Recovery	We help you architect and implement resilient backup and disaster recovery solutions as part of a comprehensive business continuity plan.
Supply Chain Security	Our Risk & Vulnerability Assessment services can be extended to your critical suppliers, helping you manage and document third-party risk.
Access Control & Authentication	We architect and implement Zero Trust security models, making strong MFA and least-privilege access a core part of your defense, directly addressing NIS2 mandates.
Vulnerability & Threat Management	Our Endpoint Security (EDR/XDR) and Network Security (NGFW, SASE) solutions provide continuous monitoring and protection against threats.

Your Next Step: From Assessment to Action

This checklist highlights the core pillars of the NIS2 Directive. The time for preparation is over; the era of NIS2 compliance is here. Whether your national laws are fully enacted or in their final stages, the obligation to meet these heightened cybersecurity standards is now a business imperative.

As your cybersecurity navigator in the Benelux region, Trescudo specializes in translating these legal requirements into a practical and effective security strategy. We help you accelerate your compliance journey, address gaps, and build a resilient program that not only meets NIS2 requirements but also protects your business from modern threats.

The time to act is now.

Contact Trescudo today for a consultation on your NIS2 strategy.

TRESCUDO

Trescudo

The Trescudo Guide to the NIS2 Directive equips Benelux businesses with a comprehensive checklist to navigate the stringent cybersecurity standards mandated by the EU's NIS2 Directive. As management assumes greater accountability for cybersecurity, this guide identifies essential requirements and helps organizations uncover compliance gaps. With Trescudo's expertise, transform regulatory challenges into actionable strategies that not only meet NIS2 obligations but also fortify your business against evolving threats.

TRESCUDO