Bachelor Computer Science & Economics

From Obligation to Action:

A Practical NIS2 Implementation Tool for SMEs in the logistics sector

Elliot Archer, s3146715

First supervisor and second supervisor:
Bas Kruiswijk & Joost Visser

RESEARCH PROPOSAL BACHELOR THESIS

Leiden Institute of Advanced Computer Science (LIACS)
www.liacs.leidenuniv.nl

08/07/2026

Abstract

The NIS2 Directive imposes cybersecurity risk-management obligations on around 300,000 entities across the European Union, yet small and medium-sized enterprises (SMEs) in the logistics sector face persistent difficulty translating these legal requirements into concrete operational steps, constrained by limited budgets, scarce cybersecurity expertise, and the complexity of the regulation. While the European Union Agency for Cybersecurity (ENISA) has published technical implementation guidance, it is formally scoped to digital infrastructure entities and functions as a compliance reference rather than a self-assessment instrument, leaving logistics SMEs without a practical way to determine where they stand. This thesis addresses that gap by developing a sector-specific self-assessment tool. The NIS2 Article 21(2) measures, as operationalised in the ENISA guidance, are extracted into 41 requirements, each translated into a single logistics-specific self-assessment question and mapped to one concrete remediation action. Each action is assigned a priority tier derived from legal criticality and implementation effort, producing a prioritised compliance roadmap. The tool is implemented as a stateless, browser-based web application that identifies an organisation's compliance gaps and generates an ordered action plan, with full traceability from each recommendation back to its regulatory source. An expert validation with logistics practitioners and a domain adviser to the sector indicated that the tool has practical value as a structuring and prioritising instrument, and informed a small set of refinements to its presentation.

Contents

1 Introduction **3**
- 1.1 Research Questions . . . 3

2 Background **4**
- 2.1 The NIS2 Directive . . . 4
- 2.2 Structure of the NIS2 Directive . . . 4
- 2.3 The Implementing Regulation and ENISA Guidance . . . 5
- 2.4 Challenges for SMEs . . . 6
- 2.5 The Logistics Sector . . . 6

3 Methodology **7**
- 3.1 Phase 1: Requirement Extraction . . . 8
- 3.2 Phase 2: Question Design . . . 9
- 3.3 Phase 3: Action Mapping . . . 9
- 3.4 Phase 5: Expert Validation . . . 11

4 Requirements **13**

5 Question Design **14**

6 Action Mapping **14**

7 Tool Implementation **15**
- 7.1 Architecture and Technology . . . 15
- 7.2 Assessment Flow . . . 16
- 7.3 Scoring and Output . . . 16

8 Validation Findings **17**

9 Tool Refinements **19**

10 Discussion **20**
- 10.1 Validity of the Tool . . . 20
- 10.2 Practical Application . . . 20
- 10.3 Limitations . . . 21
- 10.4 Future Research . . . 21

11 Conclusion **22**

References **23**

A Requirement Dataset **23**

B Question Dataset **30**

C Action Mapping Dataset **33**

D Validation Protocol **37**

E Validation Responses **39**

1 Introduction

The cybersecurity threat landscape facing European organisations has deteriorated markedly. The European Union took action and adopted the NIS2 Directive, which entered into force in January 2023 and establishes a common, elevated level of cybersecurity obligations across the European Union [Eur22]. The directive substantially broadens the scope of its predecessor, the NIS1, extending binding requirements to approximately 300,000 entities across eighteen sectors of critical importance, transport among them [Eur22].

For small and medium-sized enterprises (SMEs), however, the existence of clear legal obligations does not translate readily into practical compliance. Research indicates that organisations struggle with such requirements not because they lack motivation, but because the regulations are complex and need to be translated into concrete operational steps [BCB10]. This pattern is confirmed in the NIS2 context: a 2025 study of implementation among German SMEs found that, while larger firms in critical sectors were moderately prepared, service-oriented SMEs scored significantly lower, constrained by limited budgets, scarce cybersecurity expertise, and the complexity of risk-management and reporting requirements [JK25].

The transport sector is classified in Annex I of the directive as one of the critical sectors [Eur22]. Logistics firms are not a NIS2 category by themselves; they do however enter scope because their activities match listed entity types, most commonly as operators of Intelligent Transport Systems or as freight transport companies [Eur22]. Many of the firms captured this way are SMEs, and the literature on NIS2 barriers finds that such organisations struggle to translate the directive's requirements into concrete measures and would benefit from sector-specific tooling, designed for that purpose [MCK+25].

ENISA's technical implementation guidance offers the most comprehensive action plan of the directive's measures currently available [ENI25], yet it is neither written for nor tested against the operational reality of logistics SMEs, and it functions as a compliance reference rather than a means for an organisation to determine whether it is currently compliant.

This thesis addresses that gap by developing a sector-specific self-assessment tool that translates the cybersecurity risk-management obligations of NIS2 Article 21(2) into logistics-specific questions, identifies an organisation's compliance gaps, and generates a prioritised action roadmap for logistics SMEs that fall within the scope of NIS2. The resulting tool is validated through an expert validation with practitioners from logistics organisations and a domain adviser to the sector, and refined in response to their feedback.

1.1 Research Questions

Main research question. How can SMEs in the logistics sector that fall within the scope of NIS2 assess to what extent they meet its requirements, and what concrete steps do they need to take to become compliant?

To answer this, three sub-questions are addressed:

1. What are the NIS2 requirements for SMEs in the logistics sector?

2. How can NIS2 requirements be translated into self-assessment questions that are understandable and actionable for logistics SME practitioners?
3. How can self-assessment results be translated into a prioritised compliance roadmap for SMEs in the logistics sector?

2 Background

2.1 The NIS2 Directive

The NIS2 Directive (EU) 2022/2555 came into force in January 2023 and establishes cybersecurity requirements throughout the European Union [Eur22]. It replaces the original NIS Directive from 2016, which covered approximately 20,000 entities. NIS2 was adopted by all 27 EU Member States and applies to around 300,000 entities across 18 sectors of critical importance, including energy, healthcare, transport, and digital services. The expansion was driven by increasing cyber threats, accelerated digitalisation, and geopolitical tensions that exposed systemic vulnerabilities in European infrastructure.

NIS2 applies to any entity with 50 or more employees or more than €10 million in annual turnover operating in the specified sectors [Eur22]. The directive mandates entities to implement risk management processes, incident reporting, business continuity plans, supply chain security processes, and governance structures, with penalties of up to €10 million or 2% of global annual turnover for non-compliance.

2.2 Structure of the NIS2 Directive

The directive is organised into multiple chapters and articles, each addressing different aspects of cybersecurity regulation. Understanding this structure is essential to grasp why this thesis focuses specifically on Article 21.

Articles 1–5: Scope and Definitions. These articles define the directive's purpose, geographical scope, and key terminology. Article 1 establishes the overall objective of achieving a high common level of cybersecurity across the EU. Articles 2–4 define which sectors and entity sizes fall within scope, and set apart "essential" and "important" entities. Article 5 provides definitions for key terms used in the directive.

Articles 6–11: National Frameworks and Competent Authorities. These articles require Member States to establish national cybersecurity strategies, designate authorities responsible for supervision, and create Computer Security Incident Response Teams (CSIRTs). They define the governance structure for implementing and enforcing NIS2 at a national level.

Articles 12–19: Cooperation and Information Sharing. These articles establish rules for cross-border cooperation, information sharing between Member States, and coordination through the Cooperation Group and CSIRTs Network.

Article 20: Governance. Article 20 requires management bodies to approve cybersecurity risk-management measures, oversee their implementation, and undergo cybersecurity training. This

article assigns accountability at leadership level but does not specify what technical or operational measures must be implemented.

Article 21: Cybersecurity Risk-Management Measures. Article 21 is the operational core of the directive. It defines the minimum cybersecurity risk-management measures that entities must implement. Article 21(2) lists ten categories of measures, ranging from risk analysis and incident handling to access control and cryptography. This is the most detailed and actionable part of the directive, as it directly translates into technical and organisational capabilities that organisations must build.

Article 22: Reporting to Management. Article 22 requires entities to report on their cybersecurity posture to management bodies at regular intervals, ensuring ongoing oversight without specifying implementation details.

Articles 23–30: Incident Notification and Reporting. These articles define how entities must report significant cybersecurity incidents to national authorities. Article 23 establishes the notification timelines: a 24-hour early warning, a 72-hour detailed notification, and a final report. Article 23(3) defines a significant incident as one that "has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned."

Articles 31–39: Supervision and Enforcement. These articles grant authorities the power to supervise entities, conduct audits, and penalise entities for non-compliance.

Articles 40–46: Final Provisions. These articles address implementation timelines, review processes, and entry into force of the directive.

2.3 The Implementing Regulation and ENISA Guidance

NIS2 Article 21(5) empowers the European Commission to make the technical and methodological requirements of Article 21(2) more specific. On 17 October 2024, the Commission published Commission Implementing Regulation (EU) 2024/2690 [Eur24], which lays down these requirements in a structured Annex of 13 chapters. The regulation is legally binding for the digital infrastructure and ICT service management sectors covered by its scope, and serves as the authoritative operationalisation of Article 21(2) across those sectors.

ENISA, the European Union Agency for Cybersecurity, is the EU's dedicated cybersecurity agency, established in 2004 and strengthened by the EU Cybersecurity Act [ENI25]. Under the NIS2 framework, ENISA plays a central supporting role: it assists Member States with implementation guidance, publishes threat landscape reports, and provides practical tools to support compliance. In June 2025, ENISA published the Technical Implementation Guidance on Commission Implementing Regulation (EU) 2024/2690 [ENI25]. This 170-page document provides, for each of the 13 requirement chapters in the regulation's Annex: actionable implementation advice, examples of evidence showing that a requirement is in place, and mappings to international standards such as ISO/IEC 27001:2022 and the NIST Cybersecurity Framework 2.0.

Although the ENISA guidance is the most comprehensive action road-map of the NIS2 Article 21(2) currently available, it does not fill the gap this thesis addresses for two reasons. First, the implementing regulation and its associated guidance are scoped to digital-infrastructure entities

(cloud providers, DNS services, managed service providers, and similar organisations), not to other sectors such as transport, within which logistics operates. ENISA explicitly notes that the guidance "may provide indications" for other entities, but it is not written for or tested against the operational reality of logistics SMEs [ENI25]. Second, the document is structured as a compliance reference, not a self-assessment tool: it explains what must be done and how to evidence compliance, but does not help an organisation identify where it currently stands, which gaps are most critical, or what to prioritise given limited resources. These two limitations together create the gap that this thesis addresses.

2.4 Challenges for SMEs

Although the directive provides regulatory clarity, achieving practical compliance remains challenging for many organisations. Research consistently shows that organisations face difficulties not from lack of motivation but because regulations are complex and require translation into practical steps [BCB10]. A 2025 study on NIS2 implementation in German SMEs confirmed this pattern: while larger companies in various critical sectors demonstrated moderate compliance readiness, service-oriented SMEs scored significantly lower [JK25]. Three challenges were identified: lack of budget, lack of cybersecurity knowledge, and complexity of risk management and reporting requirements. ENISA acknowledged these challenges in their 2021 report on cybersecurity for SMEs [ENI21]. The report found that over 80% of SMEs stated a cyberattack would have serious negative consequences for their business within a week, and 57% said it would likely result in bankruptcy or closure. Despite this awareness of the risks, only 28% of surveyed SMEs had assigned a dedicated Information Security Officer role, and over 90% of SMEs that adopted new technology during the COVID-19 pandemic added no additional security measures alongside it [ENI21]. These figures come from before NIS2 and reflect conditions under a period with less strict rules, and laws; the obligations under NIS2 are substantially higher, suggesting the compliance gap has widened rather than narrowed since 2021. It should also be noted that NIS2 compliance overlaps significantly with obligations under the General Data Protection Regulation (GDPR), particularly in areas such as incident reporting, access control, and data protection measures. This overlap is relevant for logistics SMEs handling customer and freight data, but falls outside the scope of this thesis, which focuses specifically on the NIS2 Article 21(2) cybersecurity risk-management obligations.

2.5 The Logistics Sector

The transport sector is classified under Annex I of the NIS2 Directive as a sector of high criticality [Eur22]. Annex I subdivides transport into four sub-sectors: air, rail, water, and road and, for each, names the specific entity types that fall within scope. For road, these are road authorities responsible for traffic management control and operators of Intelligent Transport Systems; for water, inland waterway, maritime and coastal passenger and freight transport companies, together with port managing bodies; with comparable named entity types for air and rail [Eur22].

"Logistics" is therefore not itself a category in the directive. The label 'logistics' covers a range of activities (warehousing, freight forwarding, coordination, and transport execution), and whether a logistics firm is subject to NIS2 depends on the specific activity it performs. A logistics SME is most likely to fall within scope where its activity matches a listed entity type: for example as an operator

of Intelligent Transport Systems under the road sub-sector, or as a freight transport company under the water sub-sector [Eur22]. Parcel and courier operators are considered as important rather than essential entities as stated in Annex II [Eur22]. Activities such as pure warehousing or freight forwarding are not named in their own right, so their operators may fall outside scope unless one of these hooks applies.

Because this way of classifying is specific to each entity, the tool does not assume that every logistics firm is in scope: it opens with a scope check (Section 7) that confirms whether an organisation's activity falls within a covered sector before the assessment proceeds. The directive applies, in general, only to medium-sized and larger enterprises, those with at least 50 employees or more than €10 million in annual turnover, so the "SMEs" addressed in this thesis are specifically logistics SMEs that meet this threshold [Eur22].

The in-scope logistics SMEs facing these compliance challenges typically operate on thin margins and rely heavily on interconnected software systems, such as warehouse management systems (WMS), transport management systems (TMS), GPS tracking platforms, and customer portals, while often lacking dedicated cybersecurity staff. Research on NIS2 barriers consistently finds that SMEs struggle to interpret the directive's requirements and translate them into action, owing primarily to limited budgets and a shortage of cybersecurity expertise [MCK+25, JK25].

The choice of logistics as the target sector follows from this gap. Three considerations motivate it. First, logistics SMEs are companies reached through the critical sector transport, yet no tailored action plan exists for these entities. Second, they rely heavily on a well-defined set of software systems (WMS, TMS, telematics, GPS, carrier portals). This allows generic guidance to be worded in a way that logistics SMEs can understand and makes a self-assessment tool actionable for non-specialists. Third, the literature on NIS2 barriers identifies sector-specific, ready-to-use tooling as one of the most effective interventions for resource-constrained SMEs [MCK+25], making a single, well-defined sector the natural unit for such a tool. Selecting one sector also bounds the work: the requirements themselves come from Article 21(2) and the ENISA guidance; what this thesis contributes is the translation of those requirements into a form that logistics SMEs can understand and act on.

Despite the availability of ENISA's technical guidance, no practical self-assessment tool exists that is tailored to logistics operations. The ENISA guidance is not written for the sector, does not reference logistics-specific systems such as WMS, TMS or telematics, and does not provide a mechanism for an organisation to assess its own compliance position and generate a prioritised action plan. This thesis addresses that gap by developing a sector-specific self-assessment tool that translates NIS2's Article 21(2) obligations into logistics-specific assessment questions, identifies compliance gaps, and generates a prioritised action roadmap considering the resource constraints of logistics SMEs.

3 Methodology

This research develops a self-assessment tool through five phases: requirement extraction, question design, action mapping, tool implementation, and expert validation. The first three phases produce the datasets that power the tool (the requirements, questions, and actions) and are presented as

results in Sections 4, 5 and 6 respectively; the fourth phase, tool implementation, is described in Section 7. The fifth phase, expert validation, is designed and reasoned through below; its findings are presented in Section 8 and the resulting refinements to the tool in Section 9. This section explains the reasoning behind each design-stage phase: why it was done, how it was done, and what choices were made.

3.1 Phase 1: Requirement Extraction

Scope of Requirement Selection

This thesis focuses on Article 21 of the NIS2 Directive, which defines the cybersecurity risk-management measures that entities must implement. These are operational requirements (backup procedures, incident response plans, access controls, supply chain security) that translate directly into technical and organisational actions. This makes them well-suited for conversion into self-assessment questions and implementation steps.

Other articles were excluded for the following reasons. Article 20 (Governance) establishes high-level obligations such as management accountability and leadership training. While important, these are primarily organisational policy matters rather than implementable technical controls. Articles 23–30 (Incident Reporting) define regulatory reporting processes and timelines for communicating with national authorities. These are procedural obligations toward authorities rather than internal operational capabilities that SMEs can assess and implement independently. Articles 31–46 address supervision, enforcement, and final provisions; relevant to authorities, not to entities implementing compliance. Article 21 represents what SMEs must practically *do* to secure their systems, while other articles describe *who is responsible* and *how to communicate with authorities*.

One operational component of Article 23 is included as an exception. Article 23(1) requires entities to notify authorities of significant incidents, but the internal capability to detect and classify whether an event meets the notification threshold is an operational requirement that must be built internally. This capability is therefore included as a requirement (R10) derived from the operational reading of Article 23(1) in conjunction with the definition of a significant incident in Article 23(3).

Source for Requirement Extraction

Requirements are derived directly from Commission Implementing Regulation (EU) 2024/2690 [Eur24], as structured and interpreted in the ENISA Technical Implementation Guidance (Version 1.0, June 2025) [ENI25]. The ENISA guidance provides the authoritative operational interpretation of each requirement in the Annex to the regulation. Each requirement is mapped to a specific numbered point in that Annex (e.g. Annex §2.1.1), ensuring direct traceability to the regulatory source.

This approach eliminates subjective interpretation by the researcher: rather than translating Article 21 sub-paragraphs independently, requirements are extracted as ENISA has already defined them. Any competent authority reviewing this tool can verify each requirement against the same source. Each requirement is structured consistently using: requirement ID, ENISA guidance reference, a summary of the regulation text, an operational statement translated into logistics-specific terms, the corresponding NIS2 Article 21(2) sub-paragraph, and the relevance to logistics SMEs. The complete set of 41 requirements is provided in Appendix A.

The 41 requirements follow the structure of the ENISA guidance Annex and span all thirteen of its chapters. Chapter 13, Environmental and Physical Security, is included on the same basis as every other chapter: its three sub-headings map directly to Article 21(2), points (c), (e) and (i) [Eur24], the same sub-paragraphs already addressed by requirements drawn from other chapters of the Annex, and translate into operational controls a logistics SME can implement, such as backup power for on-site servers and network equipment, protection of the premises housing IT infrastructure, and control of physical access to server rooms or network cabinets. Requirements are not merged or removed: the count reflects the structure of the regulation itself.

3.2 Phase 2: Question Design

Each of the 41 requirements is translated into a single self-assessment question. A single question per requirement was chosen over multi-question structures because: (1) it produces an unambiguous compliance result for each requirement without combining multiple sub-scores; (2) it reduces respondent burden for logistics SME staff who may not have a cybersecurity background; and (3) it preserves direct one-to-one traceability between each regulatory obligation and the tool's output.

The answer scale of **Yes / Partial / No** allows nuanced scoring while remaining straightforward for non-technical staff. A "Yes" answer indicates the requirement is substantially met; "Partial" indicates it is partially in place but incomplete or inconsistently applied; "No" indicates the requirement is not yet met. Both "No" and "Partial" answers trigger the corresponding action in the tool's output.

Questions are deliberately phrased in operational terms specific to the logistics sector. Rather than asking whether "an incident response plan exists," the question references disruptions to warehouse management systems or tracking platforms. Rather than asking about "asset management," the question refers to servers, telematics units, and mobile scanning devices. This specificity reduces ambiguity and makes the tool immediately actionable for logistics SMEs without requiring prior knowledge of cybersecurity frameworks. The complete set of 41 questions is provided in Appendix B.

It should be noted that the tool relies on self-reported answers. A respondent may answer "Yes" to a question without the underlying control being fully effective, for example confirming that MFA is enabled without knowing that it has been misconfigured. This is an inherent limitation of self-assessment tools and is acknowledged as a boundary condition of the tool's output. The tool assesses reported compliance, not verified compliance.

3.3 Phase 3: Action Mapping

The first two phases establish *what* logistics SMEs must comply with and *whether* they comply. Phase 3 addresses the natural next step: *what to do* when the answer to a question is No or Partial.

For each of the 41 requirements, one concrete remediation action is defined. The action describes the specific step the organisation must take to move from non-compliant to compliant. Actions are derived directly from the guidance section of the ENISA Technical Implementation Guidance [ENI25], which provides indicative and actionable advice on implementing each requirement. Where the ENISA guidance offers multiple steps, the action is written as the single most direct remediation path, phrased in logistics-specific operational terms consistent with the approach used in Phase 2.

Each action is assigned a **priority tier** (Critical, Important, or Recommended) that the tool uses to order the output roadmap. The priority tier is determined by two factors: **legal criticality** and **implementation effort**.

Legal Criticality

NIS2 sets maximum fines at the level of the entity rather than the individual measure: under Article 34, infringements of Article 21 carry a ceiling of up to €10 million or 2% of global annual turnover for essential entities, and up to €7 million or 1.4% for important entities [Eur22]. In neither case does the directive differentiate between the sub-paragraphs of Article 21(2): there is no legal text stating that failure to implement MFA carries a higher fine than failure to maintain a security policy. Fine exposure alone therefore cannot differentiate the 41 requirements.

Since the directive does not assign differentiated fine levels to individual Article 21(2) requirements, legal criticality is instead derived from the *operational consequence* of non-compliance, using Article 23(3) of NIS2 as the threshold criterion. Article 23(3) defines a significant incident as one that "has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned." A requirement is classified as **High** legal criticality where its absence directly enables or substantially increases the probability of a significant incident in this sense. **Medium** criticality is assigned where absence increases risk but is not a direct enabling factor. **Low** criticality applies to governance and process requirements whose absence has an indirect rather than immediate security impact. This classification is applied systematically across all 41 requirements based on the ENISA guidance consequence statements and the researcher's analysis of each requirement's role in the security chain.

Implementation Effort

Implementation effort reflects the practical burden of performing the action, assessed from the perspective of a resource-constrained logistics SME. Effort is rated on three levels. **Low** effort means the action is achievable with existing staff and no tooling investment; primarily documentation or policy writing. **Medium** effort means the action requires process changes, staff time, or minor tooling. **High** effort means the action requires dedicated budget, technical expertise, or infrastructure changes.

This assessment is grounded in two sources. First, the ENISA Technical Implementation Guidance: requirements addressed through written policies or designated responsibilities are treated as lower effort than those requiring technical deployment or infrastructure change [ENI25]. Second, the research of Joswig and Kurz [JK25], which identifies budget constraints and lack of cybersecurity expertise as the primary implementation barriers for SMEs, meaning that requirements which demand financial investment or specialist skills are rated higher effort.

Priority Tier

The two dimensions combine into a priority tier according to the matrix in Table 1.

The decision to let legal criticality dominate is deliberate and traceable: legal criticality is derived from NIS2 Article 23(3), a fixed legal standard. Implementation effort, while practically important,

Legal Criticality	Implementation Effort	Priority Tier
High	Any	**Critical**
Medium	Low	**Important**
Medium	Medium	**Important**
Medium	High	**Important**
Low	Low	**Recommended**
Low	Medium	**Recommended**
Low	High	**Recommended**

Table 1: Priority tier matrix based on legal criticality and implementation effort.

is organisation-dependent and not a legal standard. A Critical action must be addressed regardless of cost, because its absence directly exposes the organisation to a significant incident and the associated regulatory consequences. A numeric scoring system was deliberately avoided: without empirically validated weights, any numeric formula would introduce researcher subjectivity that cannot be traced to a source. The three-tier classification is fully traceable: every tier assignment can be verified against Article 23(3) and the ENISA guidance. The complete action mapping is provided in Appendix C.

3.4 Phase 5: Expert Validation

Once implemented, the tool was evaluated through an expert validation with practitioners from logistics organisations and a domain adviser to the sector. The validation has two objectives: to test whether the tool can be used without specialist support, and to test whether logistics SMEs within the scope of NIS2 can determine where they stand against its obligations. This subsection sets out how participants were selected and how the validation was conducted; the findings themselves are presented in Section 8.

Expert Selection

Participants were selected purposively rather than at random, because the value of the validation rests on each participant's capacity to judge the tool against the operational reality of a logistics SME, rather than on statistical representativeness. The panel was composed to combine two complementary perspectives: practitioners from logistics organisations who could assess the tool against the reality of their own operation, and domain expertise from a professional adviser to the logistics sector who could assess the quality and design of the instrument itself. Selection was governed by two criteria, applied according to the participant's role.

The first criterion is *scope and sector relevance*. The intended users of the tool are SMEs in the logistics sector whose activity connects them to transport, and which therefore fall within a critical sector under NIS2, either transport under Annex I or postal and courier services under Annex II [Eur22]. NIS2 classifies an entity as in scope where it meets the size threshold of at least 50 employees or more than €10 million in annual turnover [Eur22]. Participants were drawn from organisations operating in this sector; the individual characteristics of each participating organisation, including

its size and turnover, are reported with the responses in Appendix E, since they bear on how the responses are read.

The second criterion is *comprehension*. Selecting a sector-relevant organisation is not sufficient; the participant must hold a role with enough knowledge of the organisation's IT systems and operations, or of the sector, to answer the assessment questions accurately and to judge whether the resulting action plan is meaningful and helpful, for example an owner, an operations manager, a director, the person responsible for IT, or a professional consultant to logistics organisations.

Validation Method

Companies were approached using the selection method described above, ensuring that each participating organisation and participant met the scope and comprehension criteria. Each participant was given access to the tool and then completed a structured questionnaire, provided in Appendix D. The questionnaire was sent by email so that participants used the tool independently and answered without prompting; the questions were standardised across participants to keep the responses comparable and to make clear where the tool would need to change if a problem were reported.

The questions were grouped by the research question they address, so that each part of the tool is validated against the sub-question it concerns. For SQ1, the questions test whether the requirement areas are recognisable and relevant to a logistics operation, and whether any expected obligation appears to be missing. For SQ2, they test whether the self-assessment questions are clear enough to answer without specialist knowledge, whether any are ambiguous, and whether the referenced systems (WMS, TMS, GPS tracking, telematics, carrier portals) match those the organisation actually operates. For SQ3, they test whether the Critical actions correspond to the most urgent gaps, whether the Recommended actions read as lower priority, and whether the actions are concrete and realistic for an organisation of that size. The questions addressing the main research question test whether the participant had a clearer picture of the organisation's NIS2 position after using the tool than before, and whether the tool could be used independently without guidance.

Responses were read for similarities and differences across participants: points on which participants agree are treated as the more robust findings, while singular outliers are noted and weighted accordingly. The analysis is interpretative, as no quantitative weighting is applied to individual responses.

4 Requirements

Phase 1 produced 41 requirements covering all thirteen chapters of the ENISA guidance Annex. The distribution across chapters is not uniform: the largest clusters, five requirements each, fall in Chapter 3 (Incident Handling), Chapter 6 (System Security) and Chapter 11 (Access Control), reflecting the operational detail that the ENISA guidance provides in these areas. The five incident-handling requirements all carry High legal criticality, owing to their direct connection to operational disruption. Governance-oriented chapters contribute fewer requirements: Chapter 1 (Policy) contributes four and Chapter 10 (Human Resources Security) three; these tend to carry lower legal criticality but provide the organisational foundation on which technical controls depend. Chapter 13 (Environmental and Physical Security) contributes three requirements (R39–R41), each carrying High legal criticality: loss of power, environmental damage, or unauthorised physical access to the premises housing logistics IT infrastructure can each independently cause the severe operational disruption that Article 23(3) treats as a significant incident.

Table 2 shows three example requirements to illustrate the structure. The complete dataset of all 41 requirements is provided in Appendix A.

ID	ENISA Ref.	Regulation Text	Operational Requirement	NIS2 Art.
R1	Annex §1.1.1	Policy on the security of NIS shall set out the entity's approach, be approved by management and list roles, responsibilities and topic-specific policies.	The organisation must maintain a documented, management-approved policy on the security of its network and information systems, covering all logistics IT systems (WMS, TMS, GPS platforms, customer portals).	Art. 21(2)(a)
R8	Annex §3.1.1–3.1.2	Entities shall establish an incident handling policy laying down roles, responsibilities and procedures for detecting, analysing, containing, responding to, recovering from, documenting and reporting incidents.	The organisation must maintain a documented incident handling policy covering all phases of incident response for logistics systems, with assigned roles, escalation contacts, and response templates.	Art. 21(2)(b)
R36	Annex §11.7.1–11.7.2	Entities shall ensure that users are authenticated by multiple authentication factors, with the strength of authentication appropriate to the classification of the asset accessed.	The organisation must implement multi-factor authentication (MFA) for access to critical and internet-accessible logistics systems (WMS, TMS, carrier portals, remote access).	Art. 21(2)(j)

Table 2: Example requirements (R1, R8, R36); full dataset in Appendix A.

5 Question Design

Phase 2 produced 41 self-assessment questions, one per requirement. Each question is phrased in logistics-specific operational terms and uses a Yes / Partial / No answer scale. Questions in the incident handling and access control chapters are particularly concrete, because the ENISA guidance for those chapters provides detailed operational steps that translate directly into assessable controls. Questions in the governance chapters (policy, roles, human resources) are broader, reflecting the nature of those requirements as organisational rather than technical controls.

Table 3 shows three example questions to illustrate the structure and logistics-specific phrasing. The complete dataset of all 41 questions is provided in Appendix B.

Q ID	Req. ID	Question	Answer
Q1	R1	Does your organisation have a written, management-approved policy on the security of its IT systems (e.g. WMS, TMS, GPS platforms, customer portals) that covers roles, responsibilities and the scope of systems it applies to?	Yes / Partial / No
Q8	R8	Does your organisation have a documented incident handling policy covering detection, containment, response and recovery for logistics IT systems, with assigned roles, escalation contacts and response templates?	Yes / Partial / No
Q36	R36	Is multi-factor authentication (MFA) implemented for access to critical and internet-accessible logistics systems (WMS, TMS, carrier portals, remote access)?	Yes / Partial / No

Table 3: Example questions (Q1, Q8, Q36); full dataset in Appendix B.

6 Action Mapping

Phase 3 produced 41 actions and their priority tiers. The distribution across priority tiers is as follows: 17 Critical, 13 Important, and 11 Recommended. Critical actions cluster around five areas: incident handling (R8–R11), secure configuration and patch management (R20–R23), business continuity and backups (R13–R14), access control (R31, R34–R36), and environmental and physical security (R39–R41). These clusters reflect the direct connection these controls have to operational disruption as defined in Article 23(3): a ransomware attack on a WMS with unpatched software, no incident response plan, no backups, and no MFA on remote access represents exactly the scenario the directive considers a significant incident, just as a power failure or unauthorised physical access to the room housing a logistics SME's on-site servers can independently disable the same systems. Recommended actions cluster around governance requirements (policy documents, roles, review cycles) whose absence creates indirect risk rather than immediate exposure.

Table 4 shows three example actions to illustrate the structure, including the reasoning behind their priority assignment. The complete action mapping for all 41 requirements is provided in Appendix C.

ID	Action (if No or Partial)	Legal Crit.	Effort	Priority
R8	Draft and approve an incident handling policy covering detection, containment, response and recovery for logistics IT systems, assigning named roles, escalation contacts and response templates.	High	Low	**Critical**
R14	Configure automated daily backups of WMS and TMS data to a separate offsite or cloud location, document the backup schedule and retention policy, and schedule a restoration test.	High	Medium	**Critical**
R1	Draft a written NIS security policy covering all logistics IT systems, listing topic-specific policies, roles and responsibilities, and have it formally approved and dated by senior management.	Low	Low	**Recommended**

Table 4: Example actions (R8, R14, R1); full dataset in Appendix C.

7 Tool Implementation

The preceding three phases produced the datasets that constitute the substance of this thesis: the 41 requirements (Section 4), their corresponding self-assessment questions (Section 5), and the prioritised remediation actions (Section 6). This phase operationalises those datasets as a working instrument: a web-based self-assessment tool that a logistics SME can use, without prior cybersecurity knowledge, to determine its compliance position and obtain a prioritised action plan. This section describes the tool at the level of its architecture and operation rather than its source code; the emphasis is on how the design serves the requirements established in the methodology.

7.1 Architecture and Technology

The tool is implemented as a single-page web application built with React. It runs entirely in the user's browser: there is no backend server, no database, and no account or login. An assessment exists only for the duration of a session, and no responses are transmitted or stored. This client-side design is a deliberate response to the constraints identified in Section 2.4. Logistics SMEs are sensitive about disclosing their security posture, and a tool that retained or transmitted self-declared weaknesses would discourage candid use; a stateless, browser-only tool removes that concern entirely. It also eliminates hosting and maintenance overhead; the application is served as static files and can be deployed to any static host, which keeps the instrument freely and durably accessible to resource-constrained organisations.

Internally the application separates three concerns. A data layer holds the domain content: the thirteen chapters of the ENISA guidance Annex and the 41 requirements themselves, each carrying its question, remediation action, ENISA reference, NIS2 article, legal-criticality and effort ratings, and resulting priority tier. A scoring layer transforms a set of answers into chapter scores, an overall score, and an ordered list of gaps. A presentation layer renders the sequence of screens through which the user moves. Holding the regulatory content in a discrete data layer makes the datasets from Sections 4–6 the single source of truth for the tool: the questions a user answers and the actions they receive are exactly those defined in the methodology, with no divergence between the documented instrument and the running one.

The tool is publicly available. Its complete source code is released under the MIT licence in an open repository on GitHub[1], together with a readme that describes the tool's purpose, installation and deployment, and with the licence information made explicit in the repository.

7.2 Assessment Flow

A user progresses through four stages. The tool opens on an introduction screen that states its purpose and displays the central caveat that it assesses reported rather than verified compliance (Section 5). A scope check then confirms that the organisation falls within NIS2 scope. It applies the directive's size threshold (fifty or more employees or more than €10 million in annual turnover) and confirms that the organisation's activity falls within a covered sector, whether transport under Annex I (for example, as an operator of Intelligent Transport Systems) or postal and courier services under Annex II [Eur22]. An organisation that does not meet the threshold is informed that it is not currently obliged to comply but may continue voluntarily. The assessment itself presents the 41 questions grouped by chapter, each answered on the Yes / Partial / No scale, with free navigation between chapters and a progress indicator; results become available only once every question has been answered. Finally, the results screen presents the organisation's compliance position and its prioritised action plan.

7.3 Scoring and Output

The scoring layer applies the model that follows from the single-question-per-requirement design (Section 5): a Yes counts as full satisfaction of a requirement, a Partial as half, and a No as none. These values are aggregated per chapter and expressed as a percentage of the maximum attainable, which drives a traffic-light indicator for each chapter: green for substantial compliance, amber for partial, red for weak, giving an at-a-glance map of where the organisation is strong and where it is exposed. An overall percentage summarises the position across all chapters.

The action plan is the tool's principal output and the point at which the prioritisation framework of Section 6 becomes operational. Every requirement answered No or Partial is treated as a gap and surfaced together with its predefined remediation action. Gaps are ordered by priority tier: Critical, then Important, then Recommended, so that the organisation is directed first to the controls whose absence most directly exposes it to a significant incident as defined in Article 23(3) of the directive [Eur22]. Each action is presented with its priority tier, the user's own answer, and a reference back to the originating ENISA Annex section, preserving the traceability that underpins the whole approach: every recommendation can be followed back to the regulatory source from which it was derived [ENI25]. The completed report can be exported to PDF through the browser's print function for internal use.

[1] https://github.com/Elliot-Archer/nis2-tool

Figure 1: The results screen: overall compliance score, per-chapter traffic-light indicators.

8 Validation Findings

The tool was evaluated through the expert validation described in Section 3.4. Three experts returned completed responses: a managing consultant from a logistics consultancy, a deputy managing director from an intermodal logistics organisation, and a manager from a road transport organisation. The first responded as a domain expert assessing the instrument itself; the other two as practitioners assessing the tool against their own operation. The findings are summarised here; the full responses are provided in Appendix E, and their interpretation is taken up in Section 10.

The responses converged on the tool's presentation and value. The participants who commented on

it judged it professional and well developed, and the value of a prioritised action plan relative to the full directive text was noted independently, on the grounds that few SMEs are aware of NIS2 and reading the directive itself is demanding. The tool's capacity to surface gaps an organisation believed to be already handled was reported as a concrete benefit.

The responses diverged most clearly on the main research question. The practitioner whose organisation was already engaged with NIS2 found the questions clear and the tool usable, while the practitioner encountering NIS2 for the first time did not feel the tool gave a clearer picture of the organisation's position and would not yet use it without guidance.

Three more specific points were raised. The expert participant identified one question on business continuity (Q13) as not fully clearly formulated and noted that the question list did not scroll to the top on advancing to a new chapter. One practitioner reported that the referenced IT systems did not fully match those the organisation operates, and that the tool could be shorter and more impactful. These points, and the refinements made in response to them, are addressed in Sections 9 and 10.

9 Tool Refinements

The architecture and operation of the tool are described in Section 7. The validation surfaced a small number of concrete points that could be addressed directly in the tool without altering its underlying datasets. This section sets out the refinements made in response, together with one point that, on inspection, required no change; in all other respects the tool is as described in Section 7. The 41 requirements, questions and actions were not changed, so that the one-to-one correspondence between the tool's content and the methodology set out in Sections 4 to 6 is preserved.

First, a navigation issue reported by the expert participant was corrected. On advancing to a new chapter, the question list did not return to the top of the page, so that on longer chapters the user lost their position in the assessment. The chapter navigation was adjusted so that each new chapter opens at the top of its question list, restoring orientation on chapters of any length.

Second, the expert participant noted that the business continuity question (Q13) was not fully clearly formulated and suggested making explicit that the plan should rest on an assessment of which systems are most critical and how long they can be offline. On inspection, the question already contained this clause, stating that the plan should be based on an assessment of which systems are most critical and how long they can be offline; the point is therefore recorded here as confirmation of the question's intended design rather than as a change.

Third, the system references in the question text were softened to read as illustrative rather than as a fixed list, in response to a practitioner reporting that the named systems did not fully match those the organisation operates. The named systems (WMS, TMS, GPS tracking, telematics, carrier portals) were retained as examples while making clear that equivalent systems used by the organisation are intended, so that the questions remain applicable across the range of systems found in different logistics operations.

With these refinements in place, the tool described in Section 7 constitutes the final artefact of this thesis: a self-assessment instrument that allows a logistics SME, without prior cybersecurity knowledge, to determine its compliance position against NIS2 Article 21(2) and obtain a prioritised, traceable action plan.

10 Discussion

10.1 Validity of the Tool

The validity of the tool concerns two distinct claims, which are kept apart here for clarity. The first is that the content of the tool is correct with respect to the requirements set out in NIS2 and the ENISA guidance. The second is whether the instrument is usable by its intended users, which is considered in Section 10.2.

The validity of the tool rests on its method of construction. Each of the 41 requirements is derived directly from Commission Implementing Regulation (EU) 2024/2690 [Eur24], as structured and operationalised in the ENISA Technical Implementation Guidance [ENI25], and each is then mapped to a specific point in the Annex to the regulation and to the corresponding sub-paragraph of NIS2 Article 21(2) [Eur22]. The self-assessment questions and remediation actions are in turn derived from those requirements, so that every element of the tool can be traced back to the regulatory text from which it originates. Each requirement, question and action can be checked against the same regulation and guidance, and the validity of the tool is in this way established by traceability.

10.2 Practical Application

Whereas the validity of the tool's content rests on its derivation, its practical application can be assessed only through use, and the evidence here is limited to the three validation responses, so the following observations are read as indicative rather than conclusive, with the consequences of the small panel deferred to Section 10.3.

Three tendencies emerge. First, the tool's usefulness may depend on the user's prior familiarity with NIS2: the participant whose organisation was already engaged with the directive found the questions clear and could act on the weaknesses identified, whereas the participant encountering NIS2 for the first time did not feel the tool gave a clearer picture of the organisation's position and would not yet use it unaided, which suggests, tentatively, that the tool structures existing orientation more readily than it creates it.

Second, one practitioner did not regard the Critical actions as the most urgent gaps while accepting the Recommended actions as deferrable, pointing to a tension between priority as the tool derives it from the legal standard of NIS2 Article 23(3) [Eur22] and priority as an organisation perceives its own operational urgency; this reflects not an error in the prioritisation, which is traceable to its legal basis by design (Section 3.3), but a case for communicating that basis more clearly to the user.

Third, one practitioner reported that the referenced IT systems did not fully match those the organisation operates and that the tool could be shorter and more impactful, both of which concern the presentation of the instrument rather than the correctness of its content and are consistent with the heterogeneity of logistics operations described in Section 2.5. Taken together, the responses offer tentative support for the tool as a structuring and prioritising instrument while indicating where its presentation and accessibility could be improved, though the weight they can bear is constrained by the number and composition of the participants, addressed next.

10.3 Limitations

The limitations of this thesis fall into two groups: those intrinsic to the design of the tool, and those arising from its validation.

The design imposes three boundaries, each established earlier and noted here for completeness. The tool assesses reported rather than verified compliance (Section 3.2); its prioritisation is traceable to NIS2 Article 23(3) [Eur22] but rests in part on the researcher's judgement rather than an empirically validated weighting (Section 3.3); and it is scoped deliberately to logistics, so its terminology is not intended to transfer to other NIS2 sectors without adaptation. It also addresses only the Article 21(2) obligations, and not the overlapping requirements of the General Data Protection Regulation (Section 2.4).

The validation was constrained by its panel and its method. The panel was small, comprising an in-scope logistics SME, a domain expert advising the sector, and a further logistics practitioner, which limits the extent to which the findings test the tool against its precise target population. Because the assessment was administered by email, brief or qualified answers could not be probed further (Section 3.4). For these reasons the observations on practical application in Section 10.2 are indicative rather than conclusive, and would require testing against a larger and more uniform sample of in-scope logistics SMEs before any firmer claim could be made.

10.4 Future Research

The limitations above indicate several directions for further work. The most immediate is empirical: the observations on practical application rest on a small panel and are indicative only, so the tool would benefit from field testing with a larger and more uniform sample of in-scope logistics SMEs, in which practitioners complete the assessment against their own operations and the resulting action plans are examined for usefulness. Such testing would allow the tendencies identified in Section 10.2, including the apparent dependence of the tool's value on prior familiarity with NIS2, to be confirmed or revised on a firmer basis.

A second direction concerns how the tool is developed. Rather than being validated once and then fixed, the instrument could be refined through repeated cycles of use and revision, in which feedback from each round of testing is incorporated into the questions, actions and presentation before the next. This iterative, user-driven approach would address the presentation issues raised during validation, in particular the fit of the tool's terminology to different logistics operations and the concern that the assessment could be shorter and more focused, which concern the accessibility of the instrument rather than the correctness of its content.

Finally, the scope of the tool could be extended. The single-sector focus that makes the present instrument concrete also bounds it, and the same method of derivation could be applied to other sectors within NIS2, or broadened to incorporate the overlapping obligations of the General Data Protection Regulation that were excluded here (Section 2.4), which are relevant to logistics SMEs handling customer and freight data.

11 Conclusion

This thesis set out to address a specific gap: although the NIS2 Directive imposes cybersecurity risk-management obligations on logistics SMEs, and although the ENISA guidance operationalises those obligations in detail, no instrument existed that allowed such an organisation to determine where it stands and what it must do to comply. The main research question asked how logistics SMEs within the scope of NIS2 can assess the extent to which they meet its requirements, and what concrete steps they must take to become compliant. The thesis answers this question by developing a sector-specific self-assessment tool that translates the obligations of NIS2 Article 21(2), as operationalised in the ENISA guidance, into logistics-specific questions, identifies an organisation's compliance gaps, and returns a prioritised action plan.

The three sub-questions structure this contribution. The first asked what the NIS2 requirements are for logistics SMEs; these were established as 41 requirements derived directly from Commission Implementing Regulation (EU) 2024/2690 [Eur24] and the ENISA Technical Implementation Guidance [ENI25], each traceable to a numbered point in the regulation's Annex and to a sub-paragraph of Article 21(2). The second asked how those requirements can be translated into questions that are understandable and actionable for practitioners; this was addressed by reformulating each requirement as a single self-assessment question in the operational terms of logistics, answered on a Yes, Partial or No scale. The third asked how the results can be translated into a prioritised roadmap; this was addressed by mapping each requirement to a concrete remediation action and assigning it a priority tier derived from the legal criticality standard of NIS2 Article 23(3) [Eur22] and an assessment of implementation effort, so that an organisation is directed first to the gaps that most directly expose it.

The contribution of the thesis is therefore the instrument and the method of its construction. Because every question and action can be traced back to the regulatory text from which it originates, the tool's content is verifiable against its source rather than against the researcher's interpretation, and its validity in this respect does not depend on the validation panel. The expert validation, while limited in scale, indicated that the tool has practical value as a structuring and prioritising instrument and pointed to where its presentation could be improved. Establishing its effectiveness more firmly would require the field testing set out in Section 10.4; what this thesis provides is a traceable, sector-specific instrument that gives a logistics SME, without prior cybersecurity knowledge, a concrete and defensible starting point for meeting its obligations under NIS2.

References

[BCB10] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3):523–548, 2010.

[ENI21] ENISA. Cybersecurity for smes: Challenges and recommendations. Technical report, European Union Agency for Cybersecurity, 2021. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf.

[ENI25] ENISA. Technical implementation guidance on commission implementing regulation (eu) 2024/2690 of 17 october 2024 laying down rules for the application of nis2 directive as regards technical and methodological requirements of cybersecurity risk-management measures. Technical report, European Union Agency for Cybersecurity, 2025. Version 1.0. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf.

[Eur22] European Commission. Directive (eu) 2022/2555 on measures for a high common level of cybersecurity across the union (nis2). Official Journal of the European Union, 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[Eur24] European Commission. Commission implementing regulation (eu) 2024/2690 of 17 october 2024 laying down rules for the application of directive (eu) 2022/2555 as regards technical and methodological requirements of the cybersecurity risk-management measures referred to in article 21(2). Official Journal of the European Union, 2024. https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj.

[JK25] Tobias Joswig and Wolfgang Kurz. Empirical analysis of nis2 adoption in eu smes: Challenges for critical infrastructure in germany. *Journal of Next-Generation Research 5.0*, 1(3), 2025.

[MCK+25] Konstantina Mentzelou, Panos T. Chountalas, Fotis C. Kitsios, Anastasios I. Magoutas, and Thomas K. Dasaklis. Identifying and modeling barriers to compliance with the NIS2 directive: A DEMATEL approach. *Journal of Cybersecurity and Privacy*, 5(4):97, 2025.

A Requirement Dataset

This appendix contains the full set of 41 requirements derived directly from Commission Implementing Regulation (EU) 2024/2690, as interpreted through the ENISA Technical Implementation Guidance (Version 1.0, June 2025). Each requirement is identified by its ENISA guidance reference (Annex point number), linked to the corresponding Article 21(2) sub-paragraph of the NIS2 Directive, and translated into an operational statement specific to logistics SME operations. The requirement count directly reflects the structure of the ENISA guidance Annex; no requirements have been merged or removed.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R1	Annex §1.1.1	The policy on NIS security shall set out the entity's approach, be approved by management bodies, list roles, responsibilities, topic-specific policies and documentation retention.	The organisation must maintain a documented, management-approved policy on the security of its network and information systems (NIS), covering all logistics IT systems (WMS, TMS, GPS platforms, customer portals), listing topic-specific policies and setting out roles and responsibilities.	Art. 21(2)(a)	Logistics SMEs often manage multiple interconnected platforms without a unifying security policy. An overarching NIS policy provides the governance foundation required by the regulation and sets the context for all other controls.
R2	Annex §1.1.2	The NIS security policy shall be reviewed at least annually and when significant incidents or significant changes to operations or risks occur; results shall be documented.	The organisation must review and, where necessary, update its NIS security policy at least once per year and following significant incidents or operational changes to logistics systems.	Art. 21(2)(a)	Logistics environments change rapidly (new carriers, platform integrations, route changes). Annual review ensures the policy remains aligned with actual risks rather than becoming a static document.
R3	Annex §1.2.1	Responsibilities and authorities for NIS security shall be assigned to roles, allocated to staff and communicated to management bodies.	The organisation must assign named individuals to cybersecurity roles and responsibilities (e.g. a person responsible for IT security), communicate those assignments to management, and reflect them in job descriptions.	Art. 21(2)(a)	Logistics SMEs frequently rely on informal arrangements. Without formally assigned roles, incident response and compliance oversight are left to chance, increasing risk of undetected breaches.
R4	Annex §1.2.3	At least one person shall report directly to the management bodies on matters of NIS security.	The organisation must designate at least one person who reports directly to senior management on cybersecurity matters, ensuring leadership accountability for NIS security.	Art. 21(2)(a)	Management accountability is a core NIS2 obligation. In logistics SMEs with flat structures, this ensures cybersecurity is not treated purely as an IT issue but receives management-level oversight.
R5	Annex §2.1.1–2.1.2	Entities shall establish a risk management framework, perform and document risk assessments following an all-hazards approach, produce a risk treatment plan, and have residual risks accepted by management bodies.	The organisation must implement a structured risk management process to identify, assess and prioritise cybersecurity risks to its logistics IT systems, document results in a risk treatment plan, and obtain management sign-off on accepted residual risks.	Art. 21(2)(a)	Logistics SMEs face risks across warehousing, transport and partner systems. A structured risk process ensures threats such as ransomware targeting WMS or GPS spoofing are identified and treated proportionately.
R6	Annex §2.1.4	Risk assessment results and the risk treatment plan shall be reviewed and updated at planned intervals (at least every two years) and when significant incidents or significant changes occur.	The organisation must review its risk assessment and treatment plan at least every two years, and whenever a significant incident occurs or major changes are made to logistics operations or systems.	Art. 21(2)(a)	Risk landscapes shift as logistics SMEs adopt new platforms, onboard carriers or expand geographically. Regular reviews prevent the risk treatment plan from becoming outdated.
R7	Annex §2.2.1	Entities shall regularly review compliance with their NIS security policies and topic-specific policies, and maintain an effective compliance reporting mechanism.	The organisation must periodically check that staff and systems comply with applicable security policies and procedures, and maintain a mechanism for reporting non-compliance.	Art. 21(2)(f)	Without compliance monitoring, policy violations (e.g. shared passwords, unencrypted freight data) go undetected. A lightweight monitoring process enables logistics SMEs to identify gaps before they lead to incidents.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R8	Annex §3.1.1–3.1.2	Entities shall establish an incident handling policy laying down roles, responsibilities and procedures for detecting, analysing, containing, responding to, recovering from, documenting and reporting incidents. The policy shall include an incident categorisation system, escalation plans, assigned roles, and response documentation.	The organisation must maintain a documented incident handling policy covering all phases of incident response (detection, containment, eradication, recovery) for logistics systems, with assigned roles, escalation contacts, and response templates.	Art. 21(2)(b)	Cyberattacks on WMS or GPS tracking can halt operations across the supply chain. A clear incident policy ensures disruptions are contained quickly and do not cascade to freight partners or customers.
R9	Annex §3.2.1–3.2.4	Entities shall lay down procedures and use tools to monitor and log activities on their NIS, detect anomalous events, review logs regularly for unusual trends, and protect logs from tampering.	The organisation must implement logging on critical logistics IT systems (WMS, TMS, remote access) and review logs periodically to detect anomalous or suspicious activity.	Art. 21(2)(b)	Early detection of unusual access patterns is essential for logistics SMEs, where a compromised carrier portal or WMS account could enable freight fraud or data exfiltration.
R10	Annex §3.4.1–3.4.2	Entities shall assess suspicious events to determine whether they constitute incidents and classify their severity, and act on this classification to trigger appropriate response.	The organisation must have a process for assessing and classifying security events (including deciding whether a NIS2 significant incident threshold is met) so that the correct response is triggered in a timely manner.	Art. 21(2)(b)	Logistics SMEs need to distinguish routine IT issues from reportable cybersecurity incidents. Clear classification criteria prevent both under-reaction (missing a serious breach) and over-reaction (unnecessary escalation).
R11	Annex §3.5.1–3.5.2	Entities shall respond to incidents in accordance with documented procedures, including containment, eradication and recovery stages, and shall log incident response activities.	The organisation must follow documented incident response procedures when a cybersecurity incident occurs, including steps for containment (stopping spread), eradication (removing the threat) and recovery (restoring logistics services).	Art. 21(2)(b)	An uncontained incident in a logistics WMS can spread to transport management and partner systems. Documented procedures with clear containment and recovery steps minimise operational downtime and data loss.
R12	Annex §3.6.1–3.6.2	Where appropriate, entities shall carry out post-incident reviews after recovery and use the findings to improve their NIS security approach.	The organisation must conduct a review after recovering from a significant incident to identify root causes and prevent recurrence, and feed findings back into its risk management and security policies.	Art. 21(2)(b)	Post-incident learning is critical for logistics SMEs. Recurring incidents indicate that awareness training or access controls need strengthening, which only structured reviews will reveal.
R13	Annex §4.1.1–4.1.3	Entities shall lay down a business continuity and disaster recovery plan (BCP/DRP), carry out a business impact analysis (BIA), and define recovery time and recovery point objectives.	The organisation must maintain a BCP/DRP for critical logistics operations (transport planning, shipment tracking, WMS), based on a documented BIA identifying which systems are most critical and the maximum acceptable downtime.	Art. 21(2)(c)	Even brief WMS or GPS outages can cause missed deliveries and contractual breaches. A BCP/DRP with defined recovery objectives ensures the organisation knows which systems to restore first and how quickly.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R14	Annex §4.2.1–4.2.3	Entities shall maintain backup copies of data with sufficient redundancy; backup plans shall define recovery times, completeness checks, secure offsite storage, access controls, retention periods, and restoration testing.	The organisation must take regular, complete backups of logistics system data (shipment records, routing data, WMS configurations), store them securely in a location separate from production systems, and test restoration procedures at planned intervals.	Art. 21(2)(c)	Data loss from ransomware or hardware failure can permanently disrupt logistics operations. Offsite or cloud-based backups with tested restoration procedures are the primary defence against extended operational downtime.
R15	Annex §4.3.1–4.3.2	Entities shall put in place a crisis management process addressing roles, communication channels, escalation procedures and the use of threat intelligence received from authorities.	The organisation must define a crisis management process for major cyber incidents affecting logistics operations, including who decides on operational responses, how customers and carriers are informed, and how coordination with authorities occurs.	Art. 21(2)(c)	A ransomware attack or major data breach affecting a logistics SME can rapidly escalate into a commercial crisis. Predefined communication and coordination procedures limit reputational damage and support regulatory notification obligations.
R16	Annex §5.1.1–5.1.2	Entities shall establish a supply chain security policy governing relations with direct suppliers and service providers, including criteria for selecting and contracting suppliers based on their cybersecurity practices.	The organisation must maintain a supply chain security policy that sets out how it evaluates cybersecurity risks from logistics IT suppliers and service providers (TMS vendors, freight exchanges, telematics providers), including minimum security criteria for supplier selection.	Art. 21(2)(d)	Logistics SMEs depend on numerous external platforms and services. A supplier using weak authentication or lacking patch management can introduce vulnerabilities directly into the logistics network.
R17	Annex §5.1.4	Based on the supply chain security policy and risk assessment, entities shall include cybersecurity requirements in contracts with direct suppliers and service providers, including incident notification obligations and the right to audit.	The organisation must include cybersecurity requirements in contracts with logistics IT suppliers and service providers (e.g. incident notification obligations, acceptable security standards, right to request evidence of security practices).	Art. 21(2)(d)	Without contractual cybersecurity requirements, logistics SMEs have no leverage when a supplier suffers a breach. Contractual clauses create accountability and enable the logistics SME to meet its own NIS2 obligations.
R18	Annex §5.1.6–5.1.7	Entities shall review the supply chain security policy and monitor and evaluate the cybersecurity practices of suppliers at planned intervals and when significant incidents or significant changes in the supply chain occur.	The organisation must periodically review the cybersecurity posture of its key logistics IT suppliers and service providers, at minimum at contract renewal or following a supplier-related security incident.	Art. 21(2)(d)	Supplier risk is not static. A vendor with adequate security when contracted may later become a risk. Regular review prevents accumulated supply chain risk from going unnoticed.
R19	Annex §6.1.1–6.1.2	Entities shall set and implement processes for the secure acquisition of ICT products and services, including security requirements as part of procurement, evaluation of supplier security practices, and verification before deployment.	The organisation must include cybersecurity requirements in the procurement of logistics IT systems (TMS, WMS, telematics, mobile scanning devices) and verify that new systems meet those requirements before deployment.	Art. 21(2)(e)	Procuring logistics software or hardware without security evaluation can introduce vulnerabilities from the outset. Logistics SMEs should ensure TMS and WMS vendors meet baseline security requirements before deployment.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R20	Annex §6.3.1–6.3.2	Entities shall establish, document, implement and monitor configurations for NIS using a configuration management process, and ensure default security settings are reviewed and changed where appropriate.	The organisation must document and apply secure configurations to all logistics IT systems and devices (servers, WMS clients, mobile terminals, routers), including changing default credentials and disabling unused features.	Art. 21(2)(e)	Default credentials and insecure configurations are among the most common attack vectors. Logistics SMEs with warehouse terminals or telematics devices that retain factory settings are particularly exposed.
R21	Annex §6.6.1–6.6.2	Entities shall specify and apply procedures for security patch management, ensuring timely application of security patches to address identified vulnerabilities, or documenting a risk-accepted decision not to patch.	The organisation must implement a patch management process for all logistics IT systems, ensuring security patches are applied within a defined timeframe or, where not applied, a documented risk acceptance decision is made.	Art. 21(2)(e)	Unpatched WMS or TMS software is a primary vector for ransomware and data breaches. A patch management process ensures known vulnerabilities are remediated before exploitation.
R22	Annex §6.10.1–6.10.3	Entities shall obtain information about technical vulnerabilities in their NIS, evaluate their exposure, and create and implement a remediation plan when the potential impact justifies it.	The organisation must monitor vulnerability notifications (e.g. vendor advisories) for logistics IT systems and act on those that pose material risk, including planning remediation where needed.	Art. 21(2)(e)	Logistics SMEs may not follow vendor security bulletins for their WMS or GPS platforms. Proactive vulnerability monitoring enables early response to newly discovered weaknesses before they are exploited.
R23	Annex §6.9.1–6.9.2	Entities shall protect their NIS against malicious and unauthorised software, implementing measures that detect or prevent the use of known malicious software.	The organisation must deploy anti-malware and/or endpoint protection measures on logistics IT systems and devices to detect and prevent malicious software, and keep those measures up to date.	Art. 21(2)(e)	Phishing and malware attacks targeting logistics dispatchers or warehouse operators are increasingly common. Anti-malware tools on endpoints and servers provide an essential layer of protection.
R24	Annex §7.1–7.2	Entities shall establish a policy and procedures to assess whether cybersecurity risk-management measures are effectively implemented, determining what to measure, how, when, who is responsible, and how results are used.	The organisation must have a process for periodically evaluating whether its cybersecurity measures are working effectively, including defining what will be assessed, how, and who is responsible for acting on the results.	Art. 21(2)(f)	Without effectiveness assessment, logistics SMEs cannot know whether their security investments are providing protection. Periodic measurement enables informed decisions about where to improve.
R25	Annex §7.3	The policy and procedures for effectiveness assessment shall be reviewed at planned intervals (at least every two years) and updated based on assessment findings, security test results and changes to the environment.	The organisation must review and update its effectiveness assessment process at least every two years, incorporating findings from security tests and changes to logistics systems or the threat landscape.	Art. 21(2)(f)	Assessment methods that were adequate when implemented may become insufficient as logistics operations expand or the threat environment evolves. Planned review ensures the process remains relevant.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R26	Annex §8.1.1–8.1.2	Entities shall ensure employees are aware of cybersecurity risks and apply cyber hygiene practices. An awareness programme shall be offered to all employees, covering risks, contact points and hygiene practices, repeated over time and covering new employees.	The organisation must run a structured cybersecurity awareness programme for all staff with access to logistics IT systems, covering relevant threats (phishing, social engineering, freight data protection), basic hygiene practices and who to contact in the event of a suspected incident.	Art. 21(2)(g)	Human error is the leading cause of cybersecurity incidents in logistics. A structured awareness programme helps drivers, dispatchers and warehouse operators recognise and avoid common threats.
R27	Annex §8.2.1–8.2.3	Entities shall identify employees whose roles require security-relevant skills and provide role-appropriate security training; training effectiveness shall be assessed.	The organisation must provide role-specific cybersecurity training to staff in high-risk positions (IT administrators, system owners, managers with access to sensitive freight data) and assess whether that training is effective.	Art. 21(2)(g)	Generic awareness training is insufficient for staff managing WMS access rights or configuring TMS platforms. Role-specific training ensures the most exposed employees have the skills to perform their security responsibilities.
R28	Annex §9.1–9.2	Entities shall establish a policy on cryptography defining the type, strength and quality of cryptographic measures required to protect assets, including data at rest and in transit, approved protocols and algorithms, and key management procedures.	The organisation must maintain a policy governing the use of encryption and cryptographic controls to protect logistics and customer data, both in transit (e.g. between WMS and carrier portals) and at rest (e.g. stored shipment records and personal data).	Art. 21(2)(h)	Logistics SMEs exchange sensitive freight and personal data across multiple systems. Without encryption and clear key management, this data is exposed to interception or unauthorised access.
R29	Annex §10.1.1–10.1.2	Entities shall ensure that NIS security responsibilities are addressed in personnel management throughout employment, including defining security responsibilities in terms and conditions of employment.	The organisation must ensure that cybersecurity responsibilities are reflected in employment terms for staff with access to logistics IT systems, including obligations to follow security policies and handle freight data appropriately.	Art. 21(2)(i)	Employees unaware of their security obligations are more likely to create vulnerabilities. Embedding responsibilities in employment terms creates a baseline of accountability across the logistics workforce.
R30	Annex §10.2.1–10.2.2	Entities shall, to the extent feasible, verify the background of employees and contractors before granting access to sensitive NIS or data. Verification shall be proportionate to the sensitivity of the role.	The organisation must, to the extent feasible, conduct background checks on personnel who will have access to critical logistics systems or sensitive freight and customer data, proportionate to the sensitivity of the role.	Art. 21(2)(i)	Logistics SMEs can be targeted via insider threats or social engineering of new employees. Background verification reduces the risk of intentional or negligent misuse of system access.
R31	Annex §10.3.1–10.3.2	Entities shall ensure that NIS security responsibilities and duties are managed at termination or change of employment, including return of assets and timely revocation of access rights.	The organisation must immediately revoke system access and recover assets (devices, access tokens) when an employee leaves or changes role, and include these obligations in employment or contractor terms.	Art. 21(2)(i)	Failure to revoke access promptly when a dispatcher, driver or contractor leaves is a common vulnerability in logistics SMEs. Timely offboarding prevents former employees from retaining access to WMS, TMS or carrier portals.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R32	Annex §11.1.1–11.1.2	Entities shall establish an access control policy defining rules for access to systems and data based on business and security requirements, applying need-to-know and least-privilege principles, and segregating duties where applicable.	The organisation must maintain an access control policy defining who is permitted to access which logistics systems (WMS, TMS, carrier portals, GPS platforms) and data, based on job role, applying the principle of least privilege and segregating conflicting duties.	Art. 21(2)(i)	Overly broad access rights in logistics IT systems create unnecessary exposure. Restricting access to what each role genuinely needs reduces the impact of compromised accounts or insider misuse.
R33	Annex §11.2.1–11.2.3	Entities shall provide, modify, remove and document access rights through a formal process. Access rights shall be reviewed at planned intervals and modified based on personnel changes.	The organisation must manage the full lifecycle of access rights (granting, modifying, revoking) through a documented process, and review access rights at planned intervals to remove unnecessary or outdated permissions.	Art. 21(2)(i)	Access rights in logistics SMEs often accumulate over time as staff change roles. Without a formal review process, former entitlements persist, increasing the attack surface for both external attackers and insider threats.
R34	Annex §11.5.1–11.5.2	Entities shall manage the full lifecycle of identities for NIS, ensuring unique identities per user, and managing shared or generic accounts under strict controls.	The organisation must ensure that each person accessing logistics IT systems has a unique, identifiable user account. Where shared accounts are unavoidable, strict controls must govern their use and accountability.	Art. 21(2)(i)	Shared accounts (e.g. a single WMS login for all warehouse staff) make it impossible to attribute actions to individuals, hindering incident investigation and enabling unchecked access.
R35	Annex §11.6.1–11.6.2	Entities shall implement secure authentication procedures and technologies based on access control requirements, applying state-of-the-art methods proportionate to the classification of the asset accessed, and reviewing these regularly.	The organisation must apply secure authentication to logistics IT systems, including strong password requirements proportionate to system sensitivity, and regularly review whether authentication methods remain appropriate.	Art. 21(2)(j)	Weak authentication is consistently exploited in attacks against logistics platforms. Strong passwords combined with account lockout policies are a minimum baseline, with further controls required for remote access.
R36	Annex §11.7.1–11.7.2	Entities shall ensure that users are authenticated by multiple authentication factors or continuous authentication solutions, with the strength of authentication appropriate to the classification of the asset accessed.	The organisation must implement multi-factor authentication (MFA) for access to critical and internet-accessible logistics systems, with stronger authentication requirements applied to the most sensitive systems and data.	Art. 21(2)(j)	Remote access to WMS, TMS and carrier portals without MFA exposes logistics SMEs to credential-based attacks. MFA substantially reduces the risk of unauthorised access even when passwords are compromised.
R37	Annex §12.1.1–12.1.2	Entities shall lay down rules for the classification of assets and classify assets according to those rules, taking into account confidentiality, integrity and availability requirements.	The organisation must classify its logistics IT assets (systems, data, hardware) according to their criticality and sensitivity, so that protection measures can be applied proportionately.	Art. 21(2)(i)	Logistics SMEs often treat all systems equally, diverting effort from the most critical assets. Asset classification ensures WMS, real-time tracking and customer data receive higher protection than less critical systems.

ID	ENISA Ref.	Regulation Text (summary)	Operational Requirement	NIS2 Art.	Relevance to Logistics SMEs
R38	Annex §12.4.1–12.4.3	Entities shall develop and maintain a complete, accurate, up-to-date and consistent inventory of their NIS and assets. The inventory shall be reviewed and updated regularly.	The organisation must maintain an up-to-date inventory of all IT assets used in logistics operations, including servers, workstations, warehouse terminals, mobile scanning devices, telematics hardware and key software systems.	Art. 21(2)(i)	Without a current asset inventory, logistics SMEs cannot ensure all devices are patched, monitored or protected. Untracked assets (e.g. old warehouse terminals or unauthorised personal devices) create blind spots in security coverage.
R39	Annex §13.1.1–13.1.3	Entities shall prevent loss, damage or compromise of network and information systems, or interruption to their operations, due to the failure and disruption of supporting utilities, including by considering redundancy and monitoring utility services.	The organisation must protect servers and network equipment supporting logistics IT systems (WMS, TMS, tracking infrastructure) against power failures and other disruptions to supporting utilities, using backup power arrangements where appropriate and monitoring utility status.	Art. 21(2)(c)	Warehouse and depot operations depend on continuous power for on-site servers, scanning infrastructure and cold-chain monitoring. An unplanned power loss can halt WMS and TMS operations and risks data loss on top of the immediate disruption.
R40	Annex §13.2.1–13.2.3	Entities shall prevent or reduce the consequences of events originating from physical and environmental threats, based on the results of the risk assessment, including by designing protection measures, setting control thresholds and monitoring environmental parameters.	The organisation must implement protection measures against physical and environmental threats (fire, flood, extreme temperature) for the premises housing logistics IT systems and network equipment, based on an assessment of the relevant risks, and monitor environmental conditions against defined thresholds.	Art. 21(2)(e)	Warehouses and depots carry elevated fire and flood risk from stored goods, packaging materials and heavy equipment. Environmental damage to on-site servers or network equipment can disable WMS, TMS and tracking systems for an extended period.
R41	Annex §13.3.1–13.3.3	Entities shall prevent and monitor unauthorised physical access, damage and interference to their network and information systems, including by using security perimeters, entry controls and continuous monitoring of premises.	The organisation must restrict and monitor physical access to areas where logistics IT systems and network equipment are located (server rooms, network cabinets, control rooms), limiting entry to authorised personnel and applying physical security proportionate to the organisation's premises.	Art. 21(2)(i)	Warehouses typically see high foot traffic from drivers, temporary staff and contractors. Without physical access control around server rooms or network cabinets, unauthorised individuals could tamper with or remove the equipment supporting WMS and TMS operations.

B Question Dataset

This appendix contains one self-assessment question per requirement from Appendix A, giving a total of 41 questions. Each question is designed to directly assess whether the corresponding requirement is met. The answer scale is **Yes / Partial / No**: "Yes" indicates the requirement is substantially met; "Partial" indicates it is in place but incomplete or inconsistently applied; "No" indicates it is not yet met. All questions are phrased in logistics-specific operational terms to ensure direct applicability for logistics SMEs without requiring prior cybersecurity knowledge.

Q ID	Req.	Question	Answer
Q1	R1	Does your organisation have a written, management-approved policy on the security of its IT systems (e.g. WMS, TMS, GPS platforms, customer portals) that covers roles, responsibilities and the scope of systems it applies to?	Yes / Partial / No
Q2	R2	Has the IT security policy been reviewed and, where necessary, updated within the last 12 months or after a significant incident or major operational change?	Yes / Partial / No
Q3	R3	Is there a named person or role formally responsible for cybersecurity, with those responsibilities reflected in job descriptions and communicated to management?	Yes / Partial / No
Q4	R4	Does at least one person in your organisation regularly report to senior management (director, owner or board) on cybersecurity matters?	Yes / Partial / No
Q5	R5	Has your organisation performed and documented a cybersecurity risk assessment for its logistics IT systems, and is there a risk treatment plan listing identified risks, actions and responsible persons, approved by management?	Yes / Partial / No
Q6	R6	Has the risk assessment and treatment plan been reviewed and updated within the last two years, and after any significant incident or major change to logistics operations or systems?	Yes / Partial / No
Q7	R7	Does your organisation periodically check that staff and systems comply with its security policies, and is there a mechanism for reporting non-compliance?	Yes / Partial / No
Q8	R8	Does your organisation have a documented incident handling policy covering detection, containment, response and recovery for logistics IT systems, with assigned roles, escalation contacts and response templates?	Yes / Partial / No
Q9	R9	Are activities on critical logistics systems (WMS, TMS, remote access) logged, and are logs reviewed periodically for unusual or suspicious behaviour?	Yes / Partial / No
Q10	R10	Does your organisation have a defined process for assessing whether a security event constitutes a cybersecurity incident, including criteria for determining whether NIS2 notification thresholds are met?	Yes / Partial / No
Q11	R11	When a cybersecurity incident occurs, are documented response procedures followed, covering containment (stopping the spread), eradication (removing the threat) and recovery (restoring logistics services)?	Yes / Partial / No
Q12	R12	After recovering from a significant cybersecurity incident, does your organisation carry out a post-incident review and use the findings to improve its security measures or policies?	Yes / Partial / No
Q13	R13	Does your organisation have a business continuity and disaster recovery plan for critical logistics operations (WMS, TMS, shipment tracking), based on an assessment of which systems are most critical and how long they can be offline?	Yes / Partial / No
Q14	R14	Are regular backups taken of logistics system data, stored securely in a location separate from production systems (e.g. offsite or cloud), and is restoration tested at planned intervals?	Yes / Partial / No
Q15	R15	Does your organisation have a documented crisis management process for major cyber incidents, including who makes operational decisions, how customers and carriers are notified, and how coordination with authorities is handled?	Yes / Partial / No
Q16	R16	Does your organisation have a supply chain security policy that defines how it evaluates cybersecurity risks from IT suppliers and service providers, and sets minimum security criteria for supplier selection?	Yes / Partial / No
Q17	R17	Do contracts with key logistics IT suppliers and service providers include cybersecurity requirements, such as incident notification obligations and the right to request evidence of their security practices?	Yes / Partial / No
Q18	R18	Is the cybersecurity posture of key IT suppliers reviewed at planned intervals (e.g. at contract renewal) and following significant incidents or major changes in the supplier relationship?	Yes / Partial / No
Q19	R19	Are cybersecurity requirements defined and evaluated when procuring new logistics IT systems or hardware (TMS, WMS, telematics, scanning devices), and is a security check performed before deployment?	Yes / Partial / No
Q20	R20	Are logistics IT systems and devices configured securely (e.g. default credentials changed, unnecessary services disabled), with configurations documented and consistently applied?	Yes / Partial / No
Q21	R21	Does your organisation have a patch management process ensuring security updates are applied to all logistics IT systems within a defined timeframe, or that a documented risk acceptance decision is made when patches cannot be applied?	Yes / Partial / No
Q22	R22	Does your organisation monitor vendor security advisories and vulnerability notifications for its logistics IT systems, and act on those that pose material risk with a documented remediation plan?	Yes / Partial / No

Q ID	Req.	Question	Answer
Q23	R23	Are anti-malware or endpoint protection tools deployed on logistics IT systems and devices, actively maintained and kept up to date?	Yes / Partial / No
Q24	R24	Does your organisation have a process for periodically evaluating whether its cybersecurity measures are working effectively, with defined scope, responsible persons and a mechanism for acting on results?	Yes / Partial / No
Q25	R25	Has the effectiveness assessment process been reviewed and updated within the last two years, incorporating findings from security tests, incidents or changes to logistics systems?	Yes / Partial / No
Q26	R26	Does your organisation run a structured cybersecurity awareness programme for all staff with access to logistics IT systems, covering relevant threats (phishing, social engineering, freight data protection), repeated over time and extended to new employees?	Yes / Partial / No
Q27	R27	Do staff in high-risk positions (IT administrators, system owners, managers with access to sensitive data) receive role-specific cybersecurity training, and is its effectiveness assessed?	Yes / Partial / No
Q28	R28	Does your organisation have a policy governing the use of encryption to protect logistics and customer data, covering both data in transit (e.g. between WMS and carrier portals) and data at rest (e.g. stored shipment records)?	Yes / Partial / No
Q29	R29	Are cybersecurity responsibilities reflected in employment terms for staff with access to logistics IT systems, and are staff required to acknowledge their security obligations?	Yes / Partial / No
Q30	R30	Does your organisation conduct background checks on staff who will access critical logistics systems or sensitive freight and customer data, proportionate to the sensitivity of the role?	Yes / Partial / No
Q31	R31	Are access rights to all logistics IT systems revoked and devices returned or deactivated promptly when an employee or contractor leaves the organisation or changes role?	Yes / Partial / No
Q32	R32	Does your organisation have a documented access control policy defining who is permitted to access which logistics systems and data, based on job role and the principle of least privilege, with conflicting duties segregated where possible?	Yes / Partial / No
Q33	R33	Are access rights granted and revoked through a formal documented process, and reviewed at planned intervals to remove unnecessary or outdated permissions?	Yes / Partial / No
Q34	R34	Does every person who accesses logistics IT systems have their own unique individual user account, with shared accounts subject to documented controls where unavoidable?	Yes / Partial / No
Q35	R35	Are strong authentication requirements enforced for access to logistics IT systems, proportionate to the sensitivity of the system, and reviewed periodically?	Yes / Partial / No
Q36	R36	Is multi-factor authentication (MFA) implemented for access to critical and internet-accessible logistics systems (WMS, TMS, carrier portals, remote access)?	Yes / Partial / No
Q37	R37	Has your organisation classified its logistics IT assets (systems, data, hardware) by criticality and sensitivity, and are security measures applied proportionately to that classification?	Yes / Partial / No
Q38	R38	Does your organisation maintain an up-to-date inventory of all IT assets used in logistics operations (servers, workstations, warehouse terminals, mobile devices, telematics hardware, key software), with critical assets clearly identified?	Yes / Partial / No
Q39	R39	Are servers and network equipment supporting logistics IT systems (WMS, TMS, tracking infrastructure) protected against power failures, with backup power arrangements and monitoring of utility status in place where appropriate?	Yes / Partial / No
Q40	R40	Has your organisation implemented protection measures against physical and environmental threats (fire, flood, extreme temperature) for the premises housing logistics IT systems and network equipment, based on an assessment of the relevant risks?	Yes / Partial / No
Q41	R41	Is physical access to areas where logistics IT systems and network equipment are located (server rooms, network cabinets, control rooms) restricted to authorised personnel and monitored?	Yes / Partial / No

C Action Mapping Dataset

This appendix contains the complete action mapping for all 41 requirements. For each requirement, one remediation action is defined: the concrete step a logistics SME must take to move from non-compliant (No or Partial) to compliant. Actions are derived from the ENISA Technical Implementation Guidance [ENI25] and phrased in logistics-specific operational terms.

Each action is assigned a legal criticality level (High / Medium / Low), an implementation effort level (Low / Medium / High), and a resulting priority tier (Critical / Important / Recommended). Legal criticality is based on whether absence of the control directly enables a significant incident as defined in NIS2 Article 23(3). Implementation effort reflects the practical burden for a resource-constrained logistics SME, based on the ENISA guidance complexity and the SME barriers identified by Joswig and Kurz [JK25]. The priority tier is derived from the matrix in Table 1.

ID	ENISA Ref.	Action (if No or Partial)	Legal Crit.	Effort	Priority
R1	Annex §1.1.1	Draft a written NIS security policy covering all logistics IT systems (WMS, TMS, GPS platforms, customer portals), listing topic-specific policies, roles and responsibilities, and the scope of systems it applies to. Have the policy formally approved and dated by senior management.	Low	Low	**Recommended**
R2	Annex §1.1.2	Schedule an annual policy review. Create a simple change log document recording review date, reviewer, and any changes made. Trigger an additional review immediately after any significant incident or major change to logistics systems.	Low	Low	**Recommended**
R3	Annex §1.2.1	Designate a named individual as responsible for cybersecurity (this can be an existing IT or operations manager). Add cybersecurity responsibilities to their job description and communicate the appointment to senior management in writing.	Low	Low	**Recommended**
R4	Annex §1.2.3	Establish a recurring agenda item for cybersecurity reporting at management meetings (quarterly at minimum). The designated security person prepares a short status update covering incidents, open risks, and compliance progress.	Low	Low	**Recommended**
R5	Annex §2.1.1–2.1.2	Conduct a cybersecurity risk assessment for all logistics IT systems using a structured methodology (e.g. ENISA's risk management compendium or ISO/IEC 27005:2022). Document identified risks, their likelihood and impact, and produce a risk treatment plan listing each risk, the chosen treatment, responsible person, and implementation deadline. Present results to management for sign-off.	Medium	Medium	**Important**
R6	Annex §2.1.4	Add a biennial review of the risk assessment to the organisation's calendar. Update the risk treatment plan after the review and after any significant incident or major operational change. Document each review with a date and record of changes.	Medium	Low	**Important**
R7	Annex §2.2.1	Introduce a lightweight compliance check (e.g. quarterly internal review) verifying that staff follow security policies and that systems comply with documented configurations. Log findings and report summary results to management.	Low	Low	**Recommended**
R8	Annex §3.1.1–3.1.2	Draft and approve an incident handling policy covering detection, containment, eradication, response and recovery for logistics IT systems. Assign named roles and escalation contacts for each phase. Include response templates for common scenarios (ransomware, GPS outage, WMS data breach).	High	Low	**Critical**
R9	Annex §3.2.1–3.2.4	Enable and configure logging on critical logistics systems (WMS, TMS, remote access gateways). Schedule a monthly log review (or automated alerting where tooling permits). Ensure logs are stored in a location separate from production systems and are protected from modification.	High	Medium	**Critical**

ID	ENISA Ref.	Action (if No or Partial)	Legal Crit.	Effort	Priority
R10	Annex §3.4.1–3.4.2	Define and document classification criteria for security events, including thresholds that trigger a NIS2 significant incident notification (based on Article 23(3): severe operational disruption or financial loss). Circulate the criteria to all staff responsible for IT and operations.	High	Low	**Critical**
R11	Annex §3.5.1–3.5.2	Write step-by-step response procedures for the most likely incident scenarios (ransomware, account compromise, WMS outage). Procedures must cover containment, eradication and recovery. Record all response actions in an incident log at the time of response.	High	Low	**Critical**
R12	Annex §3.6.1–3.6.2	After any significant incident, schedule a post-incident review within two weeks of recovery. Document root cause, timeline, impact, and corrective actions. Feed findings into the risk treatment plan and, where relevant, update security policies or procedures.	Medium	Low	**Important**
R13	Annex §4.1.1–4.1.3	Perform a business impact analysis (BIA) identifying which logistics systems are most critical (WMS, TMS, shipment tracking) and the maximum acceptable downtime for each. Based on the BIA, write a BCP/DRP documenting recovery procedures, responsible persons, recovery time objectives (RTOs) and recovery point objectives (RPOs).	High	Medium	**Critical**
R14	Annex §4.2.1–4.2.3	Configure automated daily backups of WMS and TMS data (including configurations and shipment records) to a secure location separate from production systems (offsite or cloud). Document the backup schedule, retention period and access controls. Schedule a restoration test at least annually and record the result.	High	Medium	**Critical**
R15	Annex §4.3.1–4.3.2	Define a crisis management process document covering: who holds decision-making authority during a major cyber incident, how customers and carriers are notified, how coordination with national authorities occurs, and how the organisation escalates internally. Ensure the relevant staff know the process exists and where to find it.	Medium	Low	**Important**
R16	Annex §5.1.1–5.1.2	Write a supply chain security policy listing all critical logistics IT suppliers and service providers (TMS vendors, freight exchanges, telematics providers). Define minimum cybersecurity criteria for supplier selection (e.g. patch management practices, incident notification capability, data encryption standards).	Medium	Low	**Important**
R17	Annex §5.1.4	Review contracts with key logistics IT suppliers. Where cybersecurity requirements are absent, add clauses covering: obligation to notify the organisation of security incidents within 24 hours, minimum security standards (e.g. use of encryption, patch management), and the right to request evidence of security practices at contract renewal.	Medium	Medium	**Important**
R18	Annex §5.1.6–5.1.7	Add a supplier cybersecurity review to the contract renewal process for all critical logistics IT suppliers. Document the review outcome and any concerns raised. If a supplier-related security incident occurs, conduct an immediate review of that relationship.	Low	Low	**Recommended**
R19	Annex §6.1.1–6.1.2	Define a short procurement security checklist for new logistics IT systems (TMS, WMS, telematics, scanning devices). Include minimum security requirements: encryption support, patch management capability, access control features. Apply the checklist to all new procurement decisions and document the outcome before deployment.	Medium	Low	**Important**
R20	Annex §6.3.1–6.3.2	Audit current configurations of logistics IT systems and devices. Change all default credentials. Disable unused ports, services and features. Document the resulting secure baseline configuration for each system type and apply it consistently to all instances.	High	Medium	**Critical**

ID	ENISA Ref.	Action (if No or Partial)	Legal Crit.	Effort	Priority
R21	Annex §6.6.1–6.6.2	Establish a patch management process defining: who is responsible for monitoring patches, how often patches are reviewed (at minimum monthly), maximum timeframe for applying critical security patches (e.g. 14 days), and the process for documenting risk acceptance when a patch cannot be applied. Apply the process to all logistics IT systems and devices.	High	Low	**Critical**
R22	Annex §6.10.1–6.10.3	Subscribe to vendor security advisories and vulnerability notifications for all key logistics IT systems (WMS, TMS, GPS platforms). Assign a named person to review new notifications monthly. For vulnerabilities rated critical or high severity, document a remediation plan within 72 hours of discovery.	High	Low	**Critical**
R23	Annex §6.9.1–6.9.2	Deploy anti-malware or endpoint protection on all logistics IT systems and devices (servers, workstations, warehouse terminals, mobile devices). Configure automatic updates for malware signatures. Document which devices are covered and schedule quarterly coverage reviews to identify unprotected assets.	High	Medium	**Critical**
R24	Annex §7.1–7.2	Define a simple effectiveness assessment process: what will be assessed (e.g. patch status, backup success rate, access rights reviews), how often (annually at minimum), who is responsible, and how findings are reported to management. Conduct the first assessment and document the results.	Low	Low	**Recommended**
R25	Annex §7.3	Schedule a biennial review of the effectiveness assessment process itself. Update the process based on findings from assessments, security tests, and changes to logistics systems. Document each review.	Low	Low	**Recommended**
R26	Annex §8.1.1–8.1.2	Design and run a structured cybersecurity awareness programme for all staff with access to logistics IT systems. Content must cover: recognising phishing and social engineering, protecting freight and customer data, basic password hygiene, and who to contact if a suspected incident occurs. Run the programme at least annually and include it in onboarding for new employees. Document attendance.	Medium	Low	**Important**
R27	Annex §8.2.1–8.2.3	Identify staff in high-risk roles (IT administrators, WMS/TMS system owners, managers with access to sensitive freight or customer data). Provide role-specific cybersecurity training covering the specific risks and responsibilities of their role. Assess training effectiveness (e.g. via short knowledge check) and keep training records.	Medium	Low	**Important**
R28	Annex §9.1–9.2	Write a cryptography policy defining: which data must be encrypted at rest (stored shipment records, customer data, credentials) and in transit (communications between WMS, TMS and carrier portals), approved encryption protocols and algorithms (e.g. TLS 1.2 or higher, AES-256), and key management procedures. Review the policy and algorithms used annually.	Medium	Low	**Important**
R29	Annex §10.1.1–10.1.2	Add a cybersecurity obligations clause to employment contracts for all staff with access to logistics IT systems. The clause should require staff to follow security policies, protect freight and customer data, and report suspected incidents. Obtain signed acknowledgement from existing staff via a brief addendum.	Low	Low	**Recommended**
R30	Annex §10.2.1–10.2.2	Define which roles require background verification (as a minimum: roles with administrator access to logistics systems or access to sensitive freight and customer data). Implement background checks proportionate to role sensitivity for new appointments to these roles. Document the process and outcomes.	Low	Low	**Recommended**
R31	Annex §10.3.1–10.3.2	Define and implement an offboarding checklist that is triggered the same day an employee or contractor leaves or changes role. The checklist must include: revocation of all system access (WMS, TMS, carrier portals, email), return or remote wipe of devices, and revocation of physical access where relevant. Assign a named person responsible for completing the checklist and keep a record of each offboarding.	High	Low	**Critical**

ID	ENISA Ref.	Action (if No or Partial)	Legal Crit.	Effort	Priority
R32	Annex §11.1.1–11.1.2	Write an access control policy defining: which roles are permitted to access which logistics systems and data, the principle of least privilege (access limited to what is needed for the role), and any duties that must be segregated. Map current roles against this policy and identify over-provisioned accounts for immediate remediation.	Medium	Low	**Important**
R33	Annex §11.2.1–11.2.3	Implement a formal access provisioning and deprovisioning process: access is granted only via a documented request and approval. Schedule an annual review of all access rights across logistics systems to identify and remove unnecessary or outdated permissions. Keep records of all access changes.	Medium	Low	**Important**
R34	Annex §11.5.1–11.5.2	Audit all logistics IT systems for shared accounts. Where shared accounts exist, convert to individual accounts with unique credentials. Where a shared account is technically unavoidable (e.g. a legacy system), document the account, implement strict controls on its use, and log all activity under that account.	High	Medium	**Critical**
R35	Annex §11.6.1–11.6.2	Define and enforce password requirements for all logistics IT systems proportionate to system sensitivity (minimum length, complexity, expiry, account lockout after failed attempts). Implement these requirements in system settings where possible. Review authentication requirements annually.	High	Low	**Critical**
R36	Annex §11.7.1–11.7.2	Enable multi-factor authentication (MFA) on all internet-accessible logistics systems and remote access solutions (WMS, TMS, carrier portals, VPN). Where MFA cannot be immediately enabled due to system limitations, document the gap as a risk acceptance and implement as the highest-priority system upgrade.	High	Medium	**Critical**
R37	Annex §12.1.1–12.1.2	Classify all logistics IT assets by criticality (High / Medium / Low) based on the impact of their unavailability on logistics operations. Apply higher protection standards to High-criticality assets (e.g. WMS servers, real-time tracking systems). Document the classification and use it as an input to the risk assessment.	Low	Low	**Recommended**
R38	Annex §12.4.1–12.4.3	Create and maintain a complete inventory of all IT assets used in logistics operations: servers, workstations, warehouse terminals, mobile devices, telematics hardware, and key software systems. Record for each asset: name, type, owner, location, and whether it is critical. Review and update the inventory at least annually and whenever assets are added or removed.	Medium	Low	**Important**
R39	Annex §13.1.1–13.1.3	Install and test backup power (at minimum a UPS, with a generator for critical operations) for servers and network equipment supporting WMS, TMS and tracking systems. Where feasible, arrange redundant utility connections and monitor utility status, with alerts for disruptions outside defined thresholds. Document the arrangements and test them at planned intervals.	High	Medium	**Critical**
R40	Annex §13.2.1–13.2.3	Assess environmental risks (fire, flood, temperature) to the premises hosting logistics IT infrastructure. Install protection measures proportionate to that risk (e.g. smoke or heat detectors, water-ingress protection, raised placement of equipment to avoid flood exposure) and define monitoring thresholds for temperature and humidity where servers are kept. Test and review these measures at planned intervals.	High	Medium	**Critical**
R41	Annex §13.3.1–13.3.3	Restrict physical access to rooms or cabinets housing logistics IT servers and network equipment to named authorised personnel, using locks or an access-control system proportionate to the organisation's size. Log and periodically review who holds access, and monitor for unauthorised physical access where feasible (e.g. via alarm or CCTV).	High	Low	**Critical**

D Validation Protocol

This appendix contains the protocol for the validation phase. The validation has two objectives: to test whether the tool is usable by its intended users without specialist support, and to test whether it enables an in-scope logistics SME to determine where it stands against its NIS2 Article 21(2) obligations. The protocol combines an eligibility screen, baseline questions asked before the participant uses the tool, and a structured questionnaire administered by email afterwards. The questions are grouped by the research question they address.

Participant eligibility

Because the tool is intended for logistics SMEs that fall within NIS2 scope, and because its output can only be assessed meaningfully by someone who understands the organisation's systems and operations, participants are screened against two criteria before inclusion:

- **Scope.** The organisation operates in transport logistics and falls within, or plausibly within, NIS2 scope; that is, it meets the size threshold (at least 50 employees or more than €10 million annual turnover); and its activity falls within a covered sector (transport under Annex I or postal and courier services under Annex II).
- **Comprehension.** The participant holds a role with sufficient knowledge of the organisation's IT systems and operations to answer the assessment questions and to judge whether the resulting action plan is meaningful (for example, an owner, operations manager, or the person responsible for IT).

Baseline (before using the tool)

- How many employees does your organisation have, and what is its approximate annual turnover?
- Which of the listed systems does your organisation operate (WMS, TMS, GPS tracking, telematics, carrier portals, customer portals)?
- Do you have a dedicated IT or cybersecurity person on staff?
- Were you aware before today that your organisation falls within the scope of the NIS2 Directive?

SQ1 What are the NIS2 requirements for SMEs in the logistics sector?

The completeness of the requirement set is established by its one-to-one derivation from the ENISA guidance Annex (Section 4); these questions therefore test the *recognisability and relevance* of those requirements to a practitioner, not their legal completeness.

- Do the requirement areas correspond to the cybersecurity obligations you understood NIS2 to place on your organisation?
- Are there any obligations you expected to see that appear to be missing?

- Are the requirements recognisable as relevant to a logistics operation such as yours, or do any seem to belong to a different kind of business?

SQ2 Can NIS2 requirements be translated into self-assessment questions that are understandable and actionable for logistics SME practitioners?

- Were the questions clear enough to answer without specialist cybersecurity knowledge?
- Were there any questions where you were unsure what was being asked, and if so which ones?
- Do the IT systems referenced in the questions (WMS, TMS, GPS tracking, telematics, carrier portals) match the systems your organisation actually uses?
- Are there any questions that seem completely irrelevant to your type of logistics operation?
- On a scale of 1 to 5, how confident are you that your answers accurately reflect your organisation's actual situation?

SQ3 How can self-assessment results be translated into a prioritised compliance roadmap for SMEs in the logistics sector?

- Do the Critical actions feel like the most urgent gaps for your organisation?
- Do the Recommended actions feel like lower priority items that could reasonably be addressed later?
- Is there any action where the assigned priority surprises you, either too high or too low?
- Are the actions described concretely enough that you know what you would need to do to implement them?
- Is there any action that feels unrealistic for a company of your size and resources?

Main Research Question How can SMEs in the logistics sector that fall within the scope of NIS2 assess to what extent they meet its requirements, and what concrete steps do they need to take to become compliant?

- Did the tool give you a clear view of which NIS2 Article 21(2) obligations you currently meet, partially meet, or do not meet?
- After completing the tool, do you have a clearer picture of where your organisation stands against NIS2 than before?
- Would you be able to use this tool independently without guidance from a researcher or consultant?
- What is the single most useful thing the tool gave you?
- What is the single most important thing you would change?

E Validation Responses

This appendix contains the full validation responses as received, structured by the questionnaire provided in Appendix D. Each participant was asked the same baseline and research-question items. Questions a participant did not answer are recorded as NaN.

Participant 1: Managing Consultant and Partner, Groenewout

Responded as a domain expert assessing the instrument rather than completing the structured questionnaire against an own organisation. The response was provided as free commentary rather than item by item; the structured items are therefore recorded as NaN, and the commentary is reproduced below.

- Overall: the tool is professional in setup, explanation and text.
- Q13 (business continuity) is not fully clearly formulated; suggested adding that the plan should be based on an assessment of which systems are most critical and how long they can be offline.
- On advancing to the next chapter, the question list does not scroll fully to the top, causing a loss of orientation except on short lists.
- The scripted descriptions of the actions are a strong feature.
- Many SMEs are unlikely to be aware of NIS2, so a questionnaire and prioritised action plan are valuable given that reading the full directive is demanding.

Question	Answer
Baseline	
How many employees does your organisation have?	NaN
Approximate annual turnover?	NaN
Which of the listed systems does your organisation operate?	NaN
Do you have a dedicated IT or cybersecurity person on staff?	NaN
Were you aware before today that your organisation falls within NIS2 scope?	NaN
SQ1: requirements	
Do the requirement areas correspond to the obligations you understood NIS2 to place on your organisation?	NaN
Are there any obligations you expected to see that appear to be missing?	NaN
Are the requirements recognisable as relevant to a logistics operation such as yours?	NaN
SQ2: questions	
Were the questions clear enough to answer without specialist cybersecurity knowledge?	NaN
Were there any questions where you were unsure what was being asked, and if so which?	Q13 unclear

Question	Answer
Do the IT systems referenced in the questions match the systems your organisation uses?	NaN
Are there any questions that seem completely irrelevant to your type of operation?	NaN
On a scale of 1 to 5, how confident are you that your answers reflect your organisation's situation?	NaN
SQ3: action plan	
Do the Critical actions feel like the most urgent gaps for your organisation?	NaN
Do the Recommended actions feel like lower priority items?	NaN
Is there any action where the assigned priority surprises you?	NaN
Are the actions described concretely enough to know what to implement?	NaN
Is there any action that feels unrealistic for a company of your size?	NaN
Main research question	
Did the tool give a clear view of which obligations you meet, partially meet, or do not meet?	NaN
After completing the tool, do you have a clearer picture of where your organisation stands than before?	NaN
Would you be able to use this tool independently without guidance?	NaN
What is the single most useful thing the tool gave you?	NaN
What is the single most important thing you would change?	NaN

Participant 2: Deputy Managing Director, HGK Logistics and Intermodal

Question	Answer
Baseline	
How many employees does your organisation have?	22
Approximate annual turnover?	≈€25M
Which of the listed systems does your organisation operate?	NaN
Do you have a dedicated IT or cybersecurity person on staff?	Yes
Were you aware before today that your organisation falls within NIS2 scope?	No
SQ1: requirements	
Do the requirement areas correspond to the obligations you understood NIS2 to place on your organisation?	NaN
Are there any obligations you expected to see that appear to be missing?	NaN
Are the requirements recognisable as relevant to a logistics operation such as yours?	NaN
SQ2: questions	

Question	Answer
Were the questions clear enough to answer without specialist cybersecurity knowledge?	Yes, partially
Were there any questions where you were unsure what was being asked?	Yes, partially
Do the IT systems referenced in the questions match the systems your organisation uses?	No, not really
Are there any questions that seem completely irrelevant to your type of operation?	No
On a scale of 1 to 5, how confident are you that your answers reflect your organisation's situation?	3.5
SQ3: action plan	
Do the Critical actions feel like the most urgent gaps for your organisation?	No
Do the Recommended actions feel like lower priority items?	Yes
Is there any action where the assigned priority surprises you?	No
Are the actions described concretely enough to know what to implement?	Yes, partially
Is there any action that feels unrealistic for a company of your size?	Yes, partially
Main research question	
Did the tool give a clear view of which obligations you meet, partially meet, or do not meet?	NaN
After completing the tool, do you have a clearer picture of where your organisation stands than before?	No, not really
Would you be able to use this tool independently without guidance?	Not for now
What is the single most useful thing the tool gave you?	NaN
What is the single most important thing you would change?	Shorter and more impactful

Participant 3: Manager, Albers Transport

Question	Answer
Baseline	
How many employees does your organisation have?	19
Approximate annual turnover?	≈€75M
Which of the listed systems does your organisation operate?	NaN
Do you have a dedicated IT or cybersecurity person on staff?	Yes
Were you aware before today that your organisation falls within NIS2 scope?	Yes
SQ1: requirements	
Do the requirement areas correspond to the obligations you understood NIS2 to place on your organisation?	Yes
Are there any obligations you expected to see that appear to be missing?	No

Question	Answer
Are the requirements recognisable as relevant to a logistics operation such as yours?	Yes
SQ2: questions	
Were the questions clear enough to answer without specialist cybersecurity knowledge?	Yes
Were there any questions where you were unsure what was being asked?	Partially
Do the IT systems referenced in the questions match the systems your organisation uses?	Yes
Are there any questions that seem completely irrelevant to your type of operation?	NaN
On a scale of 1 to 5, how confident are you that your answers reflect your organisation's situation?	5
SQ3: action plan	
Do the Critical actions feel like the most urgent gaps for your organisation?	Yes
Do the Recommended actions feel like lower priority items?	Partially
Is there any action where the assigned priority surprises you?	NaN
Are the actions described concretely enough to know what to implement?	NaN
Is there any action that feels unrealistic for a company of your size?	No
Main research question	
Did the tool give a clear view of which obligations you meet, partially meet, or do not meet?	Yes
After completing the tool, do you have a clearer picture of where your organisation stands than before?	Yes
Would you be able to use this tool independently without guidance?	Yes
What is the single most useful thing the tool gave you?	NaN
What is the single most important thing you would change?	Tool is well developed; able to act on identified weaknesses