ECSO
EUROPEAN CYBER SECURITY ORGANISATION

January 2025

WHITE PAPER

NIS2 IMPLEMENTATION: CHALLENGES AND PRIORITIES

WORKING GROUP
Cyber Threat Management

ecs-org.eu

ABOUT

The **European Cyber Security Organisation (ECSO)** is a non-profit membership-based organisation established in 2016. Uniting more than 320 stakeholders, ECSO develops a competitive European cybersecurity ecosystem that provides trusted cybersecurity solutions, advances Europe's technological independence, and unifies its cybersecurity posture. ECSO also leads the European project ECCO, supporting activities needed to develop, promote, coordinate and organise the European-level Cybersecurity Competence Community.

EMPOWERING EUROPEAN CYBERSECURITY COMMUNITIES

CONTACT

Sebastijan Čutura
Senior Manager, Industry Cybersecurity
sebastijan.cutura@ecs-org.eu

ACKNOWLEDGMENTS

Written by: Sebastijan Čutura (Senior Manager, ECSO)

We extend our sincere gratitude to the ECSO CISO Community and ECSO Member Organisations for their invaluable contributions. Their insights into NIS2 transposition across Member States and detailed case studies have significantly enriched this analysis.

CONTRIBUTING ORGANISATIONS:

CISO #Poland
Deloitte Consulting S.r.l. S.B
Elektro - Slovenija (ELES)
Körber AG
Leonardo SpA
Ministry of National Defence of the Republic of Lithuania
Nixu Oyj
Oetker-Group
S2E: Solutions to Enterprises
SAMA PARTNERS Business Solutions
Schneider Electric
Skandiabanken AB
Sopra Steria
WithSecure
Women4Cyber Italy
Women4Cyber Luxembourg
Women4Cyber Romania

Reference:
OpenKRITIS: EU NIS 2 Direktive: Cybersecurity in Kritischen Infrastrukturen

EXECUTIVE SUMMARY

The current state of NIS2 implementation reveals significant fragmentation across the European Union. As of 2nd of December 2024, only four countries - Croatia, Italy, Belgium, and Lithuania - have fully transposed the directive, with most others targeting Q1 2025 for adoption. This fragmented implementation has created substantial operational challenges, particularly for organisations operating across borders. Member States have adopted varying approaches to entity classification, sector inclusion, and size-cap thresholds, while also implementing different incident reporting classification, compliance deadlines and referencing diverse international security frameworks.

A comprehensive survey of 155 respondents from 23 countries highlights concerning gaps in organisational readiness. Nearly three-quarters of organisations lack dedicated implementation budgets, and one-third report no management involvement despite this being a legal requirement. Organisations consistently identify several key challenges: unclear implementation requirements, supply chain security concerns, incident reporting complexities, and difficulties aligning with various security frameworks. While engagement with supervisory authorities is ongoing, satisfaction levels remain moderate, with organisations expressing a strong desire for better communication and practical guidance.

The sectoral case studies analysis reveals distinct patterns in NIS2 implementation approaches across different industries. Organisations with previous regulatory experience (such as NIS1 or sector-specific regulations) demonstrate more mature implementation strategies, while newly regulated sectors face steeper adaptation curves. Common themes emerge across sectors: the importance of leveraging existing security frameworks, the challenge of integrating multiple compliance requirements, and the varying levels of cybersecurity maturity affecting implementation approaches.

The impact on SMEs through supply chain provisions, despite being outside the direct scope, requires careful consideration. Moreover, medium-sized enterprises that are directly in the scope face disproportionate resource allocation challenges compared to larger organisations.

The findings emphasise the critical need for harmonisation across Europe to address the current fragmentation in scopes, tiering, and implementation approaches. Recommendations include establishing consistent EU-wide implementation approaches, creating standardised templates and reporting mechanisms, developing harmonised risk management frameworks, and providing targeted support for disadvantaged entities.

CONTENTS

KEY TAKEAWAYS

1.

TAKEAWAY 1

Disproportionate Impact on Medium Sized Enterprises

Medium-sized enterprises face distinct challenges under NIS2 that larger corporations are better equipped to handle. The financial impact is particularly acute when considering both the technology investments and the needed changes in the processes. While technology is crucial, establishing and maintaining effective security processes is equally important, as they ensure consistent security operations, incident response, and risk management across the organisation. Larger corporations might already have advanced security systems and mature processes in place, but medium-sized enterprises often need to build these capabilities from scratch. For instance, implementing 24/7 security monitoring or establishing secure supply chain management systems - including both the technical solutions and the supporting processes like staff training, incident response procedures, and governance frameworks - represents a much larger percentage of a medium-sized company's operating budget compared to a large corporation's resources. Moreover, while NIS2 primarily targets medium and large companies through its size-cap threshold, smaller enterprises are increasingly finding themselves indirectly affected through supply chain provisions. Essential and important entities within NIS2's scope have the authority to designate their suppliers, including SMEs, as critical to their operations. This designation allows them to enforce equivalent security requirements on these smaller suppliers, effectively extending NIS2's reach beyond its formal scope. As a result, many SMEs that fall below the size threshold may still need to implement comprehensive security measures to maintain their business relationships with larger entities covered by NIS2. This creates an additional layer of complexity and financial burden for smaller businesses that may not have anticipated falling under such stringent security requirements. These businesses essentially face the same obligations as larger companies but must meet them with significantly fewer resources and less organisational flexibility.

TAKEAWAY 2

Disproportionate Impact on Multinational Companies

Unlike local companies that only deal with one set of regulations and one authority, multinationals must juggle relationships with multiple national cybersecurity authorities, each interpreting and enforcing NIS2 in slightly different ways. For example, a security incident affecting operations in France, Germany and Spain would require coordinated reporting to three different authorities under three different national implementations of NIS2.

TAKEAWAY 3

Disproportionate Impact on Sectors with Lower Cybersecurity Maturity Level

Sectors with lower cybersecurity maturity face a particularly steep challenge under NIS2 because they're essentially being asked to make a giant technological leap forward in a short time. These sectors, which often include traditional industries like manufacturing have historically operated with basic IT systems and minimal cybersecurity measures because their core operations weren't originally designed with digital threats in mind. Now, NIS2 requires them to rapidly develop sophisticated cybersecurity capabilities that more digitally mature sectors have built gradually over many years. The challenge becomes more complex because these sectors often rely on legacy systems and operational technology that wasn't designed with modern cybersecurity features in mind.

TAKEAWAY 4

Disproportionate Impact on Newly Introduced Entities in the Scope

The newly introduced entities under NIS2 face unique implementation challenges because they're entering a complex regulatory framework without the benefit of experience from the original NIS directive. Regulatory inclusion creates particular stress points around resource allocation and expertise development. Many of these organisations have traditionally focused their investments on operational efficiency and physical security rather than cybersecurity. Now they must quickly redirect significant resources to develop digital security capabilities, often without clear industry-specific frameworks or established best practices to follow. For instance, a waste management company that previously focused primarily on physical operations must now implement sophisticated cyber risk management systems and incident reporting protocols, despite having limited experience with such requirements.

TAKEAWAY 5

NIS2 Scope & Classification Disharmony

While NIS2 provides a foundational two-tier classification system, Member States are adopting varying approaches in three critical areas: entity classification (ranging from single-tier to three-tier systems), sector coverage (with some states expanding scope), and size-cap thresholds. This regulatory fragmentation means organisations may face different compliance requirements across jurisdictions, even when providing identical services. For instance, a medium-sized company might need to comply with stringent security measures in one country while being exempt in another.

TAKEAWAY 6

International Security Framework Diversity

Countries are taking distinctly different approaches to incorporating recognised frameworks - from direct references in guidance documents to creating hybrid national standards that blend multiple frameworks. A notable example is Belgium's approach, where ISO 27001 certification is considered equivalent to meeting NIS2 requirements, setting a precedent for framework recognition. While NIST and ISO standards emerge as the most commonly referenced frameworks, supplemented by ENISA's Security Measures Reference Document for EU-specific alignment, the varying recognition and interpretation of these standards across member states creates compliance complexity for cross-border organisations.

TAKEAWAY 7

NIS2 Incident Reporting: Timeline and Classification Variances

NIS2 establishes foundational reporting timeframes (24 hours for initial reports, 72 hours for detailed follow-ups), Member States are adopting significantly different notification timeframes, with some requiring initial incident reports within 6 hours compared to NIS2's baseline 24-hour requirement. Furthermore, Member States are expanding beyond NIS2's focus on "significant" incidents by introducing multi-tiered classification systems, meaning an incident's reporting requirements could vary significantly across jurisdictions. This regulatory fragmentation is further complicated by asynchronous implementation timelines, where incident reporting requirements may take effect at different times across Member States, and variations in legal terminology defining reporting triggers.

TAKEAWAY 8

Budget Readiness: Investment Gap in Organisational Preparedness

Survey data indicates that approximately 75% of organisations have not allocated dedicated financial resources for NIS2 implementation. Some organisations may find their existing cybersecurity practices already substantially align with NIS2 requirements, reducing the need for additional dedicated funding. Others might be in the early stages of their NIS2 planning process, conducting impact assessments and gap analyses before making specific budget allocations. However, there remains a risk that some organisations are underestimating the resources needed for full implementation or struggling to prioritise cybersecurity investments within their operational budgets.

TAKEAWAY 9

Management Engagement: Critical Gap Between Regulatory Requirements and Current Practice

Survey data shows that while 66% of organisations report management engagement in their NIS2 implementation efforts, a concerning 34% indicate no management involvement. This division is particularly noteworthy given NIS2's explicit requirements for management accountability. The directive establishes cybersecurity as a board-level responsibility, mandating specific management obligations including the approval of cybersecurity measures, participation in regular training, and active implementation oversight. The substantial proportion of organisations reporting no management involvement suggests a critical gap in understanding or implementing NIS2's governance requirements. This situation not only indicates potential compliance risks but also highlights a deeper challenge in elevating cybersecurity from an IT-centric concern to a strategic business priority, as envisioned by the directive.

RECOMMENDATIONS

2.

The following recommendations for the NIS2 implementation are derived from detailed transposition analysis, practitioner survey responses, and sectoral case studies. These recommendations represent consolidated industry feedback and expert insights from the field.

RECOMMENDATION 1

Continuously **engage with a wide range of stakeholders** including public administration, sectoral and cybersecurity associations, via awareness-raising sessions, public consultations, and webinars as it ensures that practical challenges and sector-specific needs are understood and addressed early. This continuous dialogue helps create more effective and realistic compliance approaches while building trust between regulators and regulated entities through regular interaction and feedback loops.

RECOMMENDATION 2

Designate **one single point for reporting of all cybersecurity incidents, beyond the NIS2 scope**. A unified incident reporting point would significantly streamline the compliance process and reduce the administrative burden on organisations, particularly those operating across multiple sectors or jurisdictions. This centralization would eliminate confusion about where and how to report different types of cybersecurity incidents.

RECOMMENDATION 3

Standardise templates and data formats, especially focusing on incident reporting, with clear definitions to facilitate international communication & problem solving. Common definitions and reporting structures would not only speed up incident response times but also facilitate better trend analysis and threat intelligence sharing across the EU, ultimately improving the collective cybersecurity posture.

RECOMMENDATION 4

Develop a European Risk Management Framework, methodology, and open-source tool, commonly adopted across EU countries. This would create consistency in how organisations across the EU assess and manage cybersecurity risks, making it easier to implement and verify compliance requirements. This unified approach, supported by open-source tools, would be particularly beneficial for organisations operating in multiple EU countries and would help establish a baseline for cybersecurity practices across the union.

RECOMMENDATION 5

Develop a Harmonised EU Supply Chain Security Framework. A harmonised European framework for supply chain security is critical in today's interconnected business environment. Rather than having different approaches across member states, the EU should establish common baseline security measures and assessment criteria that all organisations can follow. This standardized framework would provide clear, consistent guidelines for assessing and managing supply chain risks across the EU, while establishing minimum security requirements that suppliers must meet to work with essential and important entities. Through a unified assessment methodology, it would reduce duplicate efforts when suppliers work with multiple customers in different member states, enabling mutual recognition of supply chain security assessments across the EU. This would help organisations efficiently evaluate their exposure through third parties while ensuring a consistent level of security across the European supply chain ecosystem.

RECOMMENDATION 6

Rely on existing standards as a sufficient proof of compliance. Recognising existing standards as proof of compliance would reduce redundant certification efforts and costs, while leveraging well-established security frameworks that organisations may already follow. This approach would particularly benefit organisations that have already invested in implementing international standards, allowing them to focus resources on addressing any gaps specific to NIS2 requirements.

RECOMMENDATION 7

Create an interactive table **mapping NIS2 security measures to international standards** (e.g., ISO, NIST). Creating a comprehensive mapping between NIS2 requirements and international standards would help organisations understand how their existing security controls align with NIS2 requirements and identify gaps that need addressing. This mapping would simplify compliance planning and reduce duplication of effort, particularly for organisations already certified against major international standards.

RECOMMENDATION 8

Provide targeted support for disadvantaged entities (e.g., timelines, financial incentives for implementation). Targeted support for disadvantaged entities recognises that not all organisations have equal resources or capabilities to implement NIS2 requirements within the same timeframe. This approach would help ensure a more equitable implementation of the directive while preventing security gaps that could arise from organisations struggling to meet requirements due to resource constraints.

RECOMMENDATION 9

Establish a **centralised European information hub providing an overview of NIS2 transposition status and highlighting key differences** across countries. This would significantly reduce the complexity of understanding and tracking different national implementations of NIS2, making it easier for organisations operating across multiple EU countries to ensure compliance.

INTRODUCTION

3.

More than a month after the NIS2 transposition deadline of October 18, 2024, the efforts towards its implementation are fully underway. Different types of stakeholders are involved: EU institutions are working on the definition of guidelines; Member States are working on the transposition and implementation of the Directive, often through consultations with the national entities in scope; and last, affected entities have already invested resources to better understand the scope of the Directive and its operational impact for their implementation.

The NIS2 Directive is expected to have long-term positive effects on the cybersecurity posture of entities within its scope and their environments, ultimately increasing the overall cyber resilience of European countries and society as a whole. Among main features the Directive expands the range of affected sectors, mandates comprehensive risk management measures, and requires organisations to refine their incident response plans for effective collaboration with national Computer Security Incident Response Teams (CSIRTs).

However, progress in implementing NIS2 remains highly fragmented, both at the Member State level and among individual affected entities. While some organisations are ahead of the curve and are making minor adjustments to align with national laws, others are still uncertain whether they fall within the directive's scope. Similarly, some Member States have successfully adopted NIS2 into the national legislation while majority missed the transposition deadline.

The European Commission is taking active steps in the implementation, and it has recently published an Implementing Act targeting digital infrastructures, digital providers, and ICT service management (business-to-business) sectors that will establish rules for two key aspects:

1. The technical and methodological requirements for cybersecurity risk management measures.
2. Further specification of the criteria for determining when an incident is considered significant.

ENISA is also providing active support and has recently published technical guidance to support EU Members states and NIS2 entities with the implementation of the technical and methodological requirements of the NIS2 cybersecurity risk management measures outlined in the above mentioned Implementing Act.

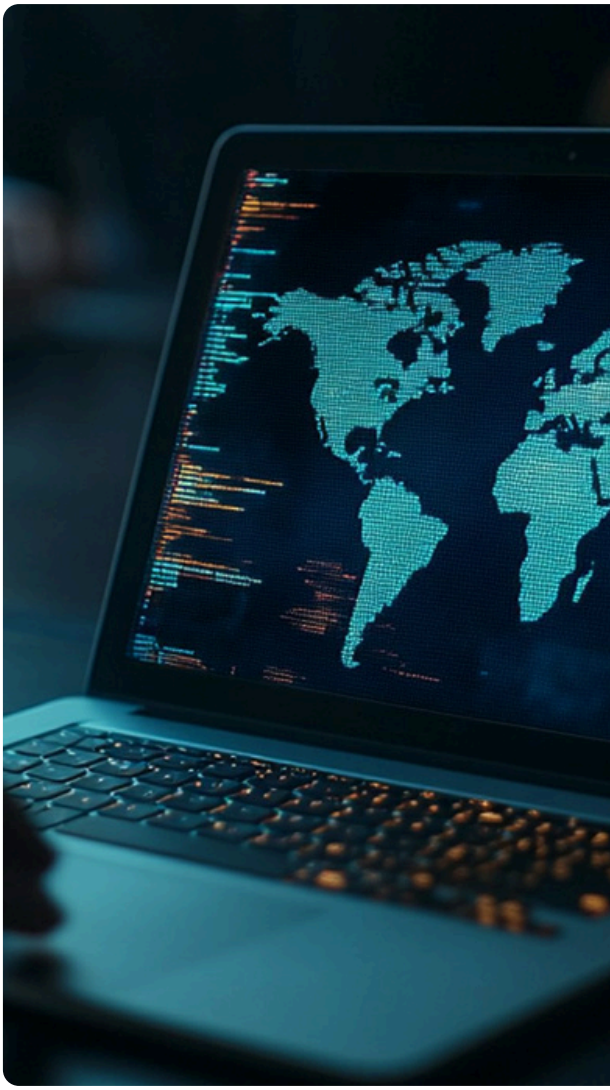
The European Cyber Security Organisation (ECSO) has actively participated in this process by submitting consolidated feedback gathered from its extensive member base in response to the Implementing Act Public Consultation.

This White Paper examines the NIS2 Directive implementation, focusing on three pillars:

1. **NIS2 Transposition Overview:** This section provides a comprehensive look at how the NIS2 Directive is being incorporated into national legislation across Member States with a focus on the differences in the approaches.

2. **Practitioner's Survey:** Survey conducted among cybersecurity professionals and affected organisations, offering insights into their preparedness and attitudes towards NIS2 implementation.

3. **Sectoral Case Studies:** Key takeaways of implementation efforts in selected sectors affected by NIS2, analysing their unique challenges and approaches.



The White Paper examines the notable similarities and contrasts in Member State implementation strategies and organisation's readiness. The analysis yields key insights, presented as actionable recommendations. These findings will prove invaluable to public administration officials, cybersecurity leaders, and a broader audience interested in understanding the current NIS2 Implementation landscape.

This White Paper seeks as a final outcome to:

- Support the efforts of all actors involved in the NIS2 implementation
- Stimulate public discourse on critical issues that are already becoming apparent
- Contribute to a more effective and coordinated approach to the implementation of EU's cybersecurity policies across Europe

NIS2 TRANSPOSITION OVERVIEW

4.

The state of transposition of the NIS2 Directive varies significantly across countries. At the time of publishing, only four countries have fully transposed NIS2 into their national law. The EU started on 28 November open infringement procedures by sending a letter of formal notice to 23 Member States calling for full transposition of the NIS2. As an EU directive, NIS2 sets out goals that all EU member states must achieve but allows each country some flexibility in how they implement those goals into their national laws. However, following the minimum harmonisation principle, countries cannot implement less stringent measures than those outlined in NIS2. For example, Member states can expand the list of sectors or entities covered by the directive in their national implementation or set stricter deadlines for incident reporting.

This analysis focuses on several areas of NIS2 identified as particularly impactful:

- Status of the EU Member State NIS2 Adoption
- Enlarged Scope and Layered Entity Classification
- Diverse International Security Frameworks
- Stricter Entity Obligations for Incident Reporting
- Timelines Divergences

Our analysis examines key differences in how various countries are approaching NIS2 implementation. Rather than providing an exhaustive comparison, the focus is on notable variations and examples in national approaches that could create significant challenges for organisations operating across borders. Comparative analysis examines NIS2 implementation across member states at different stages of their adoption process.

Disclaimer: The analysis is based on information available as of 2nd December 2024. As the implementation of NIS2 is still ongoing and Member States are in the process of transposing the Directive into national legislation, some aspects discussed in this text may be subject to change. Readers are encouraged to verify the most current requirements and interpretations as they become available through official channels.

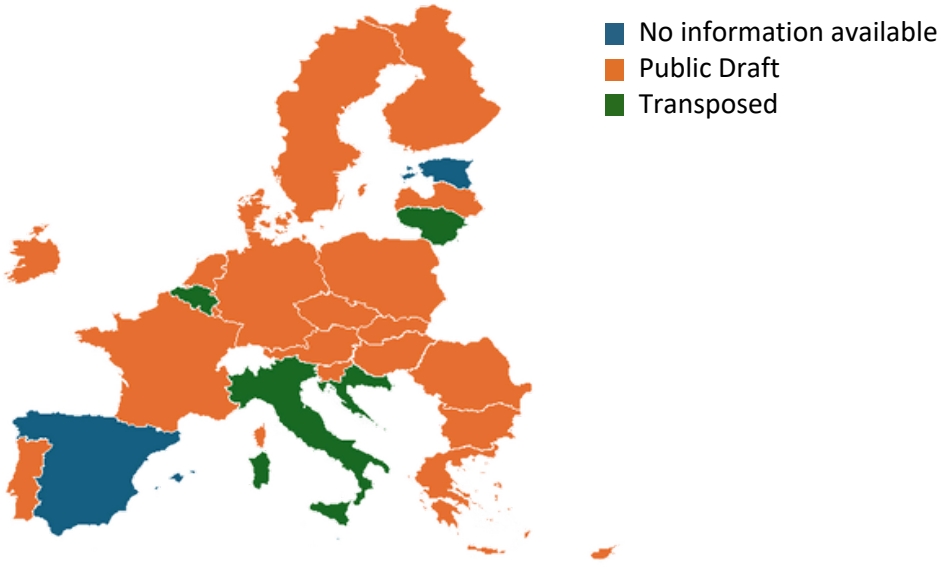


Figure 1 *Status of the EU Member State NIS2 Adoption*

Croatia, Italy, Belgium, and Lithuania are the only countries that have fully transposed NIS2 at the time of writing of this paper. A large number of countries that published drafts of the law expect to adopt NIS2 in Q1 2025.

Countries are citing various reasons for potential delays including complexity of the transposition process, requirement to adopt multiple cybersecurity policies at the same time (e.g. DORA, CER), the large-scale impact on the companies and national political factors. A notable example is the case of Austria where the National Council rejected the first version of the NIS2 which resulted in the country missing the transposition deadline. Beside the fragmentation, an additional problem for entities in scope is the lack of accessible relevant information online and the missing central repository providing an up-to-date overview of the transposition status across countries.

4.1 Enlarged Scope and Layered Entity Classification

Added intermediaries in the ICT sector, public administration and education.

Added gas, oil, coal and mineral extraction to the essential services. The draft amendment expands the scope of the regulation by classifying all providers of managed cybersecurity services (regardless of their size) as key entities. The draft amendment also includes in the group of essential entities entities indicated in Annex 2 to the Act, which exceed the requirements for a medium-sized enterprise.

Entities fall into 3-tier security levels – security measures depend on the level. Added public transport, manufacturing of cement, lime, and plaster. Public Administration not listed.

3-tier entity categorization system and lowered thresholds for affected companies, potentially encompassing businesses with fewer than 50 full time employees.

Included various levels of public administration and additional entity types like in-house compliance.

About 150 entities categorised as strategically important and added military industry.

Singular classification diverges from EU NIS2 by consolidating affected entities into one category.

The implementation of NIS2 across member states reveals significant variations that could create compliance challenges for organisations operating in multiple countries. While NIS2 establishes a baseline two-tier classification system (Essential and Important Entities), member states are adopting diverse approaches that deviate from this standard. Some countries are implementing a simplified single-tier system, while others are creating more complex three-tier classifications. This divergence becomes particularly significant when considering that security requirements are tied to these classification levels. For example, a company might need to meet more stringent security measures in one country compared to another, even though they're providing identical services.

Some member states are expanding the scope of NIS2 by including additional sectors not originally specified in the directive. This creates scenarios where an organisation might fall under NIS2 regulations in one country but remain outside the scope in another. Similarly, certain countries are lowering the size-cap thresholds that determine which organisations must comply with the directive. This means a medium-sized company might face mandatory compliance in one jurisdiction while being exempt in another.

Conversely, some countries have explicitly excluded certain sectors from their NIS2 implementation. Belgium and Finland, for example, have omitted the banking and financial market sectors from their national laws, as these are already covered by the separate DORA regulation. Hungary has notably left public administration out of its National Law implementation.

Key challenges

Inconsistent sector classification creates operational inefficiency and market inequality where organisations must maintain higher security standards (and bear associated costs) in countries that include their sector.

4.2. Diverse International Security Frameworks

Specific security measures framework similar to ISO27001 and mapping that correlates with ISO27001 and NIST SP 800-53.

National framework similar to ISO 27001 but also considers ENISA's Security Measures Reference Document.

National "Cyber Fundamentals Framework" based on NIST CSF, ISO 27001/27002, CIS Controls and IEC 62443.

Proposal is standard agnostic but supporting document explain that National and ENISA guidelines along with NIST, ISO 27001/27002, CIS Controls, and GDPR should be used.

National Framework "Nazionale per la Cybersecurity e la Data Protection", which is based on the NIST Cybersecurity Framework but adapted to the Italian context.

Framework based on ISO 27001 and NIST SP 800-53.

Countries are incorporating internationally recognised security frameworks in different ways: some reference them in supporting documentation, others create hybrid national frameworks combining elements from multiple standards, and in specific cases like Belgium, compliance with certain standards (ISO 27001) is deemed equivalent to meeting NIS2 requirements.

Among these frameworks, NIST and ISO emerge as the most frequently referenced standards, reflecting their comprehensive approach to cybersecurity and risk management. Additionally, countries often incorporate ENISA's Security Measures Reference Document to ensure alignment with EU-specific guidelines, while also considering GDPR for data protection aspects. Less frequently mentioned are CIS Controls that provide prioritised sets of cybersecurity best practices that organisations can implement, while IEC 62443 specifically addresses the unique security requirements for industrial automation and control systems.

Creating an interactive mapping table between various security frameworks could serve as a crucial tool for cross-border compliance. For example, if a company has already invested significantly in implementing ISO 27001 in one country, a detailed mapping could show them exactly which NIS2 requirements in another country are already covered by their existing controls, and what additional measures, if any, they need to implement. However, creating such equivalence isn't just about matching control frameworks - it requires careful consideration of how different countries interpret and enforce these requirements. A harmonised approach to framework recognition among member states could significantly simplify NIS2 compliance.

Currently, we see different member states favoring different frameworks - for instance, Belgium's acceptance of ISO 27001 as proof of compliance. However, rather than requiring organisations to adapt to different frameworks for each jurisdiction, member states could establish mutual recognition agreements. This would mean that compliance with any recognised framework (whether ISO 27001, NIST, or others) that meets NIS2's core requirements would be accepted across all member states. Such an approach would maintain security standards while reducing the compliance burden, especially for organisations operating across multiple EU jurisdictions

Key challenges

Companies must maintain different documentation sets, security controls, and audit processes to satisfy essentially the same security requirements across different member states.

4.3. Stricter Entity Obligations for Incident Reporting

Requires an early warning within 6 hours of incident detection.

Significant incidents can be classified as Large-scale Cyber Incidents or Crisis based on cross-border impact and severity.

Distinguishing between "incidents," "critical incidents," and "serious incidents".

Changed the wording that can be interpreted as "when detecting a significant incident" instead of "becoming aware".

Specified a 9-month grace period after entities are notified of their inclusion in the list of essential and important entities.

Expanded the scope of reportable incidents beyond just those deemed significant.

The divergence from NIS2's baseline reporting timeframes represents a significant challenge. While the directive establishes standard deadlines of 24 hours for initial reports and 72 hours for detailed follow-ups, some countries have dramatically shortened these timeframes to as little as 6 hours for initial notifications. For organisations operating across multiple countries, this creates a particularly demanding environment where they must maintain different reporting procedures and timelines for each jurisdiction.

The complexity extends beyond just timing requirements. Although NIS2 focuses on "significant" incidents, member states are expanding their scope to include additional types of reportable events. Some countries have introduced multi-tiered incident classifications, creating scenarios where an incident considered significant in one jurisdiction might fall into a different category in another.

The implementation timeline adds another layer of complexity. Countries are adopting different schedules for when incident reporting requirements take effect, which may not align with their broader NIS2 implementation dates. Furthermore, variations in legal terminology regarding incident reporting triggers – when exactly an organisation must report an incident – create uncertainty about compliance obligations.

Key challenges

The divergent scope of reportable incidents across countries, with some requiring reporting beyond just significant incidents and others applying different cross-border impact criteria, forces companies to implement broader monitoring capabilities and maintain country-specific incident response procedures, leading to increased resource requirements and compliance risks.

4.4. Timeline Divergences: by when do entities need to be compliant?

One year from the receipt of the notification on categorisation to implement security measures.

From October 18 2024 organisations need to implement security measures. Mandatory Audit by 31 December 2025.

Organisations to implement security measures by September 2026.

One year after the registration confirmation.

18 months after end of the registration period.

12 months to comply with the main requirements and 24 months to the first third party audit

After a country adopts NIS2 into the national law, the first critical deadline typically involves entity registration. This registration period varies significantly across member states, ranging from just one month to up to five months. Most countries have adopted a self-registration approach, where organisations must proactively register themselves through dedicated authorities platforms. However, Croatia and Lithuania stand out by taking a different path - these countries have chosen to actively identify and notify entities that fall within the scope of NIS2.

After receiving notification on categorisations, organisations must pay particular attention to the timeline for implementing security measures. This timeline varies significantly between countries as visible in the table above ranging from few months to more than one year.

Key challenges

Companies must either align with the earliest deadline across all jurisdictions or manage a complex matrix of country-specific timelines, significantly impacting resource allocation and compliance planning.

PRATICTIONER'S SURVEY

5.

Through a comprehensive survey spanning multiple sectors and countries, valuable insights were gained into the challenges and key priorities organisations face in their implementation journey.

Survey was conducted among **155 respondents from 23 European countries**. The survey respondents represent a broad spectrum of large, internationally operating organisations across various NIS2 sectors, with responses primarily coming from senior cybersecurity professionals.

Organisation size: The majority of respondents (63) come from large organisations with 1,000-10,000 employees. There's also significant representation from very large companies with over 25,000 employees (28) and medium-sized companies with 250-1,000 employees (19).

Sectors: The survey covers a wide range of NIS2 sectors, with Manufacturing (28 respondents), Transport (22 respondents), Energy (20 respondents), and ICT Service Management (20 respondents) being the most represented.

Geographic distribution: The respondents' organisations are headquartered across various European countries, with Spain (32), Belgium (26), and Germany (12) being the top three.

International vs. National operations: A significant majority (102 out of 155, or about 66%) of the respondents' organisations operate internationally.

Respondent roles: The majority of respondents (58%) hold CISO (Chief Information Security Officer) positions, with another 28% being part of CISO teams (including managers of Risk, Compliance, Architecture, Products, etc.). This indicates that the survey responses come primarily from cybersecurity professionals directly responsible for NIS2 implementation.

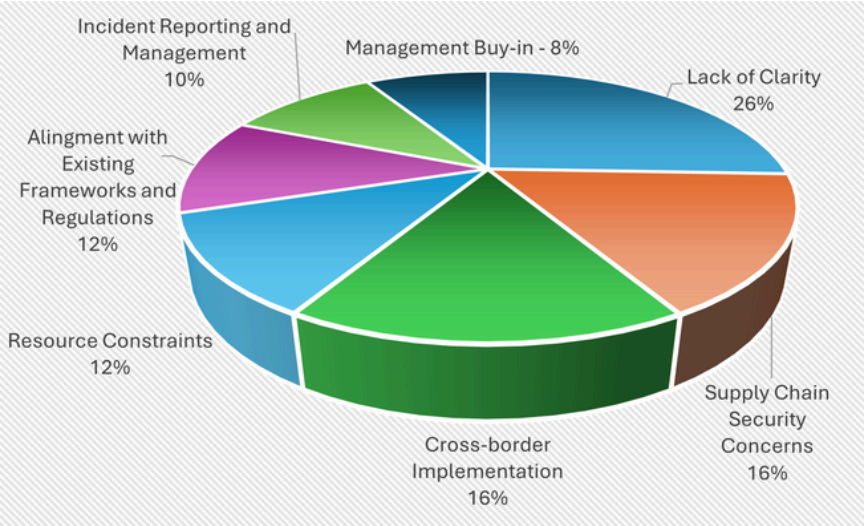


Figure 2 *What are the main challenges in the NIS2 Implementation from your organisation's perspective?*

The following graph features frequency of mentioned challenges in respondent's answers. The analysis of NIS2 implementation challenges reveals a hierarchy of critical concerns that organisations prioritize above other potential issues in their compliance journey. At the forefront, the lack of clarity in implementation requirements emerges as the most pressing challenge, indicating that organisations are primarily grappling with understanding and interpreting the directive's requirements before they can even begin addressing other aspects.

Frequently mentioned in the various parts of the Survey, respondents mentioned supply chain security as a major concern. Organisations are finding it challenging to ensure and verify the cybersecurity practices of their suppliers and partners, especially given the complex nature of modern supply chains and burdensome process of security questionnaires. Furthermore, organisations are concerned about having sufficient resources (budget, personnel, and expertise) to implement NIS2 requirements.

Organisations are grappling with how to integrate NIS2 requirements with existing cybersecurity frameworks and other regulations. They indicate challenges in aligning NIS2 with frameworks like ISO 27001 and regulations like GDPR or DORA. Several responses highlight concerns about new incident reporting obligations, including understanding what constitutes a reportable incident, meeting stringent reporting timelines, and managing the reporting process across multiple countries.

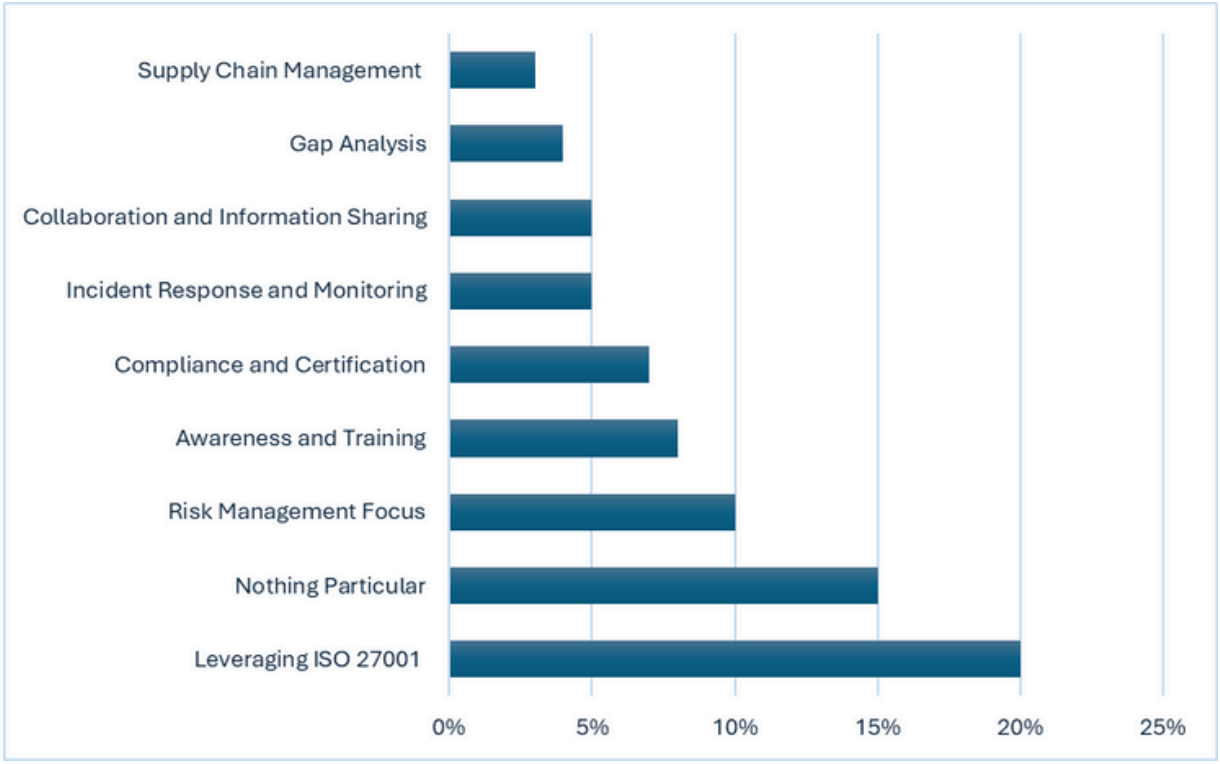


Figure 3 *If you were in the scope of the NIS1, could you please share best practices that can be applied for the transitition to the NIS2? (Frequency of mentioned best practices)*

Approximately 20% of respondents mentioned ISO 27001 or ISO standards as a best practice or recommendation for transitioning to NIS2. Around 10% of responses emphasized the importance of risk management, assessment, or prioritisation based on risk. Approximately 8% of respondents highlighted the need for continuous awareness, training, or education programs. About 7% of responses mentioned broadly compliance with specific standards or obtaining certifications. 5% of responses focused on incident response planning, notification, or continuous monitoring. Approximately 5% of respondents emphasised collaboration with authorities, other organisations, or information sharing as best practices. About 4% of responses suggested performing a gap analysis or assessment to identify areas for improvement.

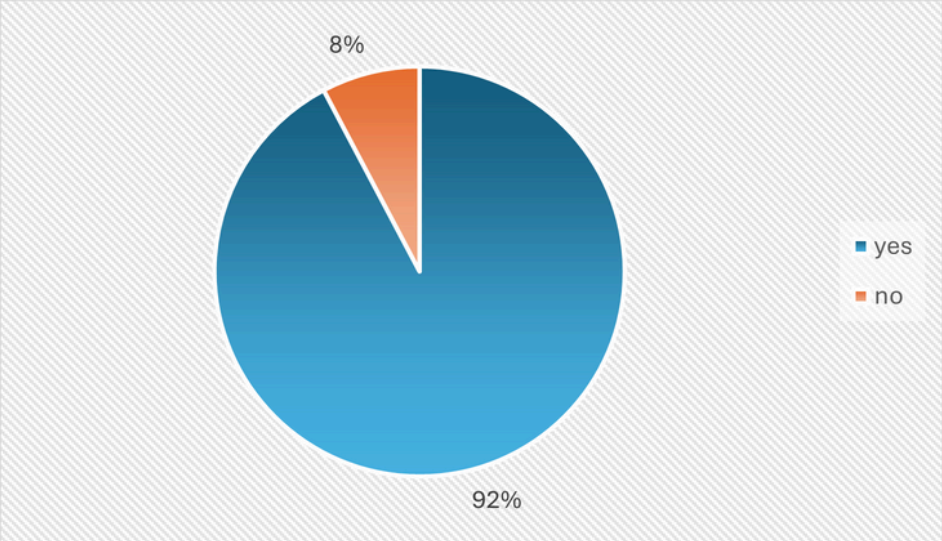


Figure 4 *Would you benefit from access to standardised guidelines, templates or other supporting materials to facilitate compliance with the NIS2?*

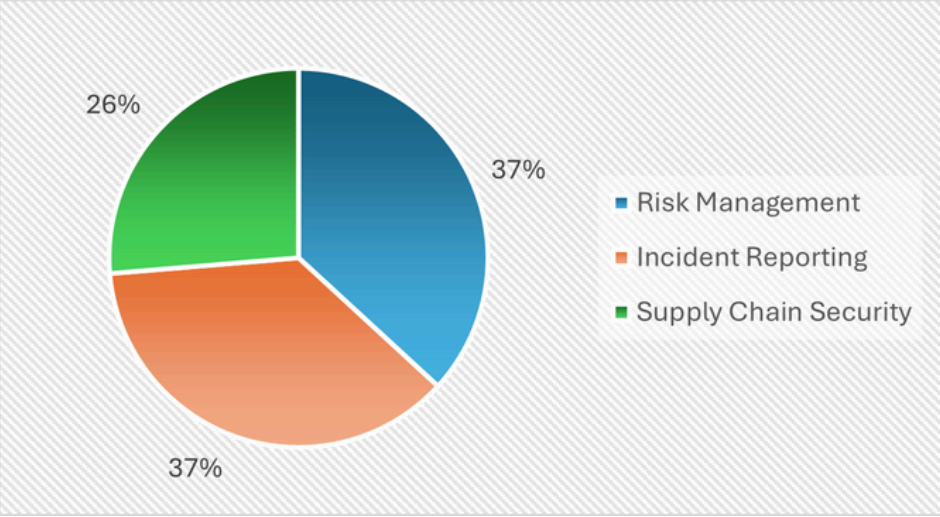


Figure 5 *Indicate the type of document and required content that would help you*

There's a clear need for practical, actionable guidance on implementing NIS2 together with standardised approaches. Aligned with the responses on main challenges, respondents mainly mention templates for Risk Management, Incident Reporting and Supply Chain Security. There's significant interest in understanding how NIS2 aligns with existing cybersecurity frameworks, particularly ISO 27001. Countries like Belgium (Cyber Fundamentals Framework), Finland (Kybermittari) and Spain (Pillar) offer structured approaches to risk assessment. The significance of these tools extends beyond their immediate practical value. They represent a shift toward standardised, accessible approaches to cybersecurity risk assessment, making it easier for organisations - especially those with limited resources - to evaluate their security posture. These national tools also serve as potential models for other member states developing their own implementation support mechanisms. While some respondents ask for high-level guidelines, others request very specific tools like risk registers or detailed checklists. Some responses indicate a need for sector-specific guidance, particularly in areas like OT (Operational Technology) environments.

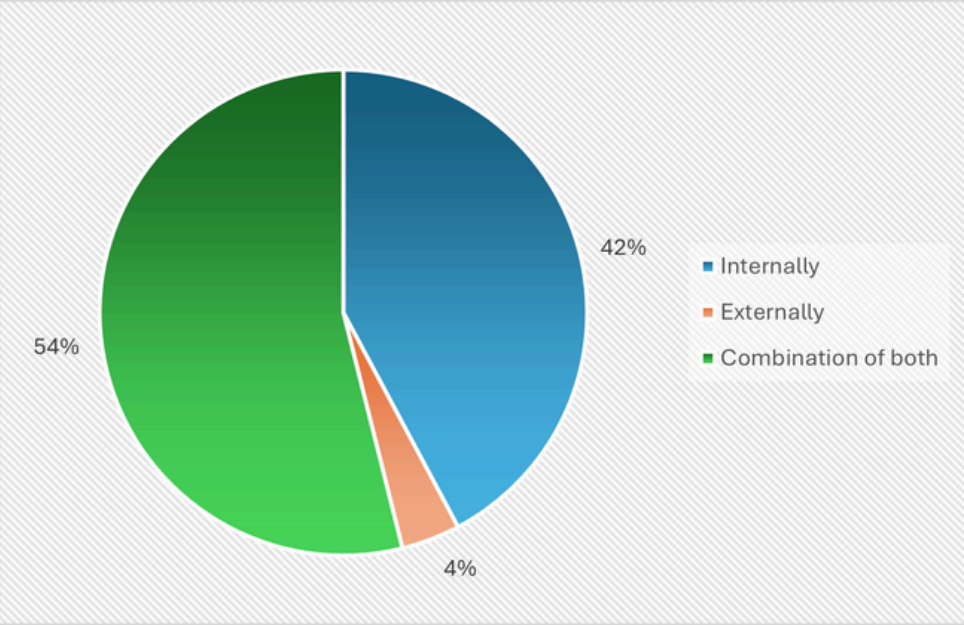


Figure 6 *Is the NIS2 Implementation conducted internally or with the support of external organisations?*

The vast majority of organisations (96%) are involving internal resources in some capacity and only a small fraction (4%) are relying solely on external support. The high number of organisations handling NIS2 implementation internally or with a combination approach suggests that many companies have some level of in-house expertise or are looking to build it. Since this directive requires ongoing compliance rather than one-time implementation, developing in-house expertise becomes more cost-effective and sustainable in the long run. The fact that over half of organisations are using a combination approach suggests they're taking a balanced path: leveraging their internal knowledge while bringing in external expertise for specialized aspects or validation.

Very few organisations are completely outsourcing the implementation, which may reflect the strategic importance of NIS2 compliance and the need for deep organisational involvement.

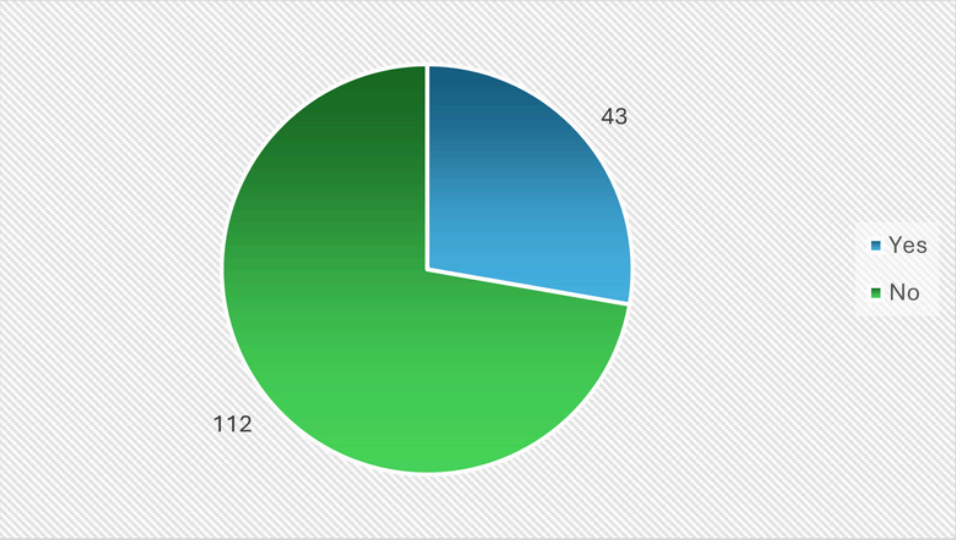


Figure 7 *Do you have a dedicated budget for the NIS2 Implementation?*

The survey data reveals a concerning preparedness gap in the NIS2 implementation, as nearly three-quarters of organisations haven't set aside specific funds for meeting the directive's requirements. This widespread lack of dedicated budgeting suggests many organisations may be underestimating the resources needed or are struggling to prioritise cybersecurity investments. The fact that only about 28% of organisations have allocated specific funds indicates a potential risk of rushed or inadequate implementation as deadlines approach, especially considering the comprehensive cybersecurity measures and organisational changes that NIS2 demands. This could indicate that NIS2 is being viewed as an extension of existing cybersecurity efforts rather than a standalone initiative. Furthermore, the lack of dedicated budgets for 72% of organisations could suggest that either:

- NIS2 requirements align closely with existing cybersecurity practices for many organisations.
- Organisations are still in early stages of planning for NIS2 implementation.
- There's a potential underestimation of the resources required.

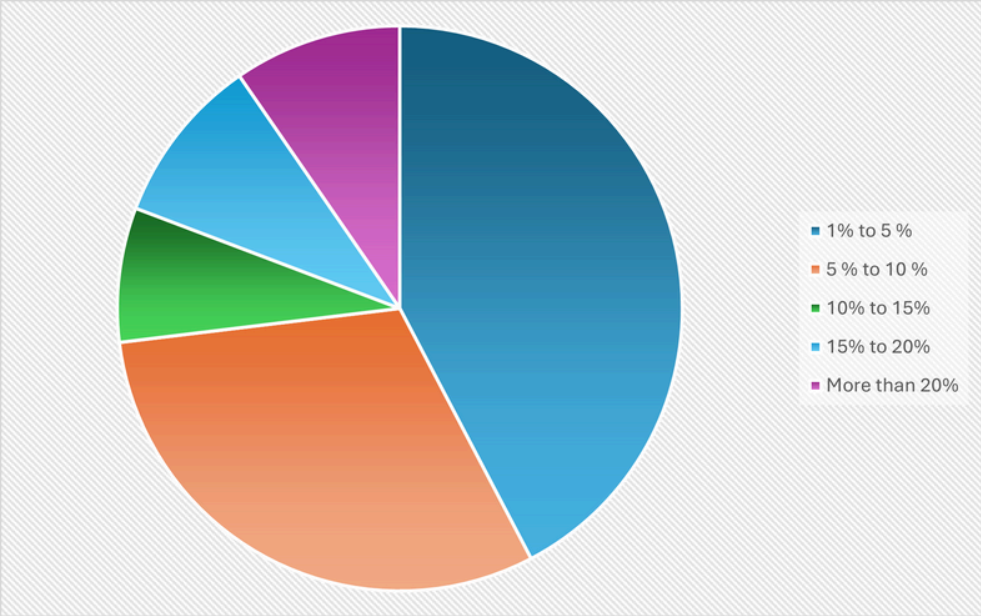


Figure 8 *If yes, could you please indicate the financial value reserved for the NIS2 (as % of the total cybersecurity budget)?*

Among those with a dedicated budget, the majority (73%) are allocating up to 10% of their total cybersecurity budget for NIS2 implementation. The most common allocation is in the 1-5% range, indicating a relatively modest budgetary commitment for many organisations. What's particularly noteworthy is the distribution at the higher end of the spectrum. A combined 30% of organisations are planning to dedicate more than 10% of their cybersecurity budget to NIS2, with some even allocating over 20%. This significant variation in budget allocation likely reflects different starting points in terms of existing cybersecurity maturity - organisations with less mature security programs may need to invest more heavily to achieve compliance. These diverse budget allocations also suggest varying interpretations of what NIS2 compliance will require, possibly reflecting the current uncertainty around specific national implementations of the directive.

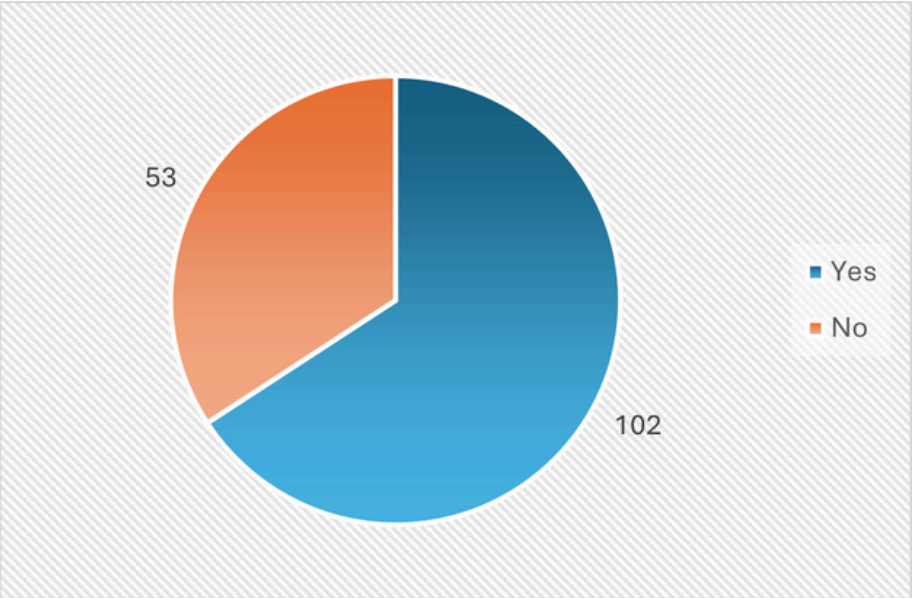


Figure 9 *Is the top management involved in the NIS2 Implementation?*

102 respondents (66%) report management involvement in NIS2 implementation, while 53 respondents (34%) indicate no management involvement. This split becomes particularly significant when we consider NIS2's explicit requirements for management engagement. Given these requirements, the fact that 34% of organisations report no management involvement is concerning. This suggests that a significant portion of organisations may not yet be aligned with NIS2's management accountability requirements. The directive specifically aims to ensure cybersecurity is treated as a board-level responsibility, not just an IT department concern. The directive mandates that management bodies must approve cybersecurity measures, undergo regular training, and maintain active oversight of implementation - making management involvement not just beneficial but legally required.

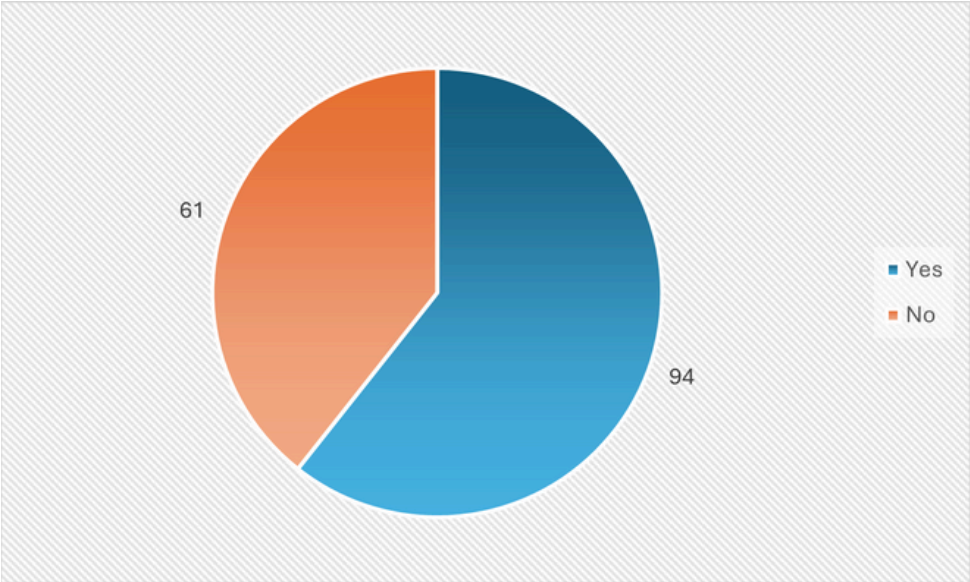


Figure 10 *Have you been in contact with national supervisory authorities with regards to the NIS2 Implementation?*

Over 60% of respondents have had some form of contact with national supervisory authorities but when respondents were asked to rate collaboration with authorities, the score is modest 6.59 out of 10 which means the quality and effectiveness of these interactions may not be meeting all their needs. The level of engagement is especially significant when considering that supervisory authorities play a crucial role in providing guidance, clarifying requirements, and ensuring consistent implementation of NIS2. Organisations that have established early contact are likely better positioned to understand and adapt to their national interpretation of the directive.

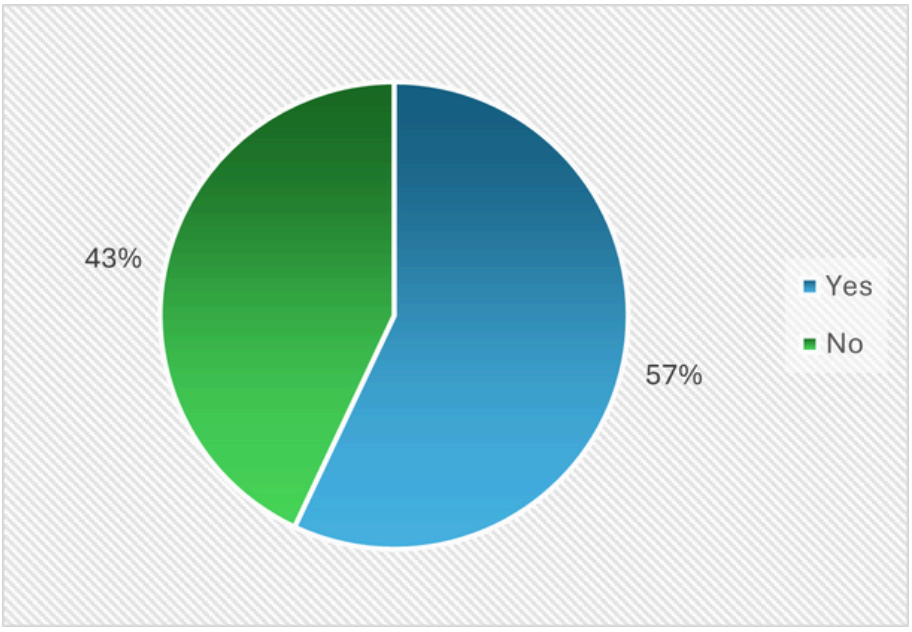


Figure 11 *Does your country organise events to raise awareness about NIS2?*

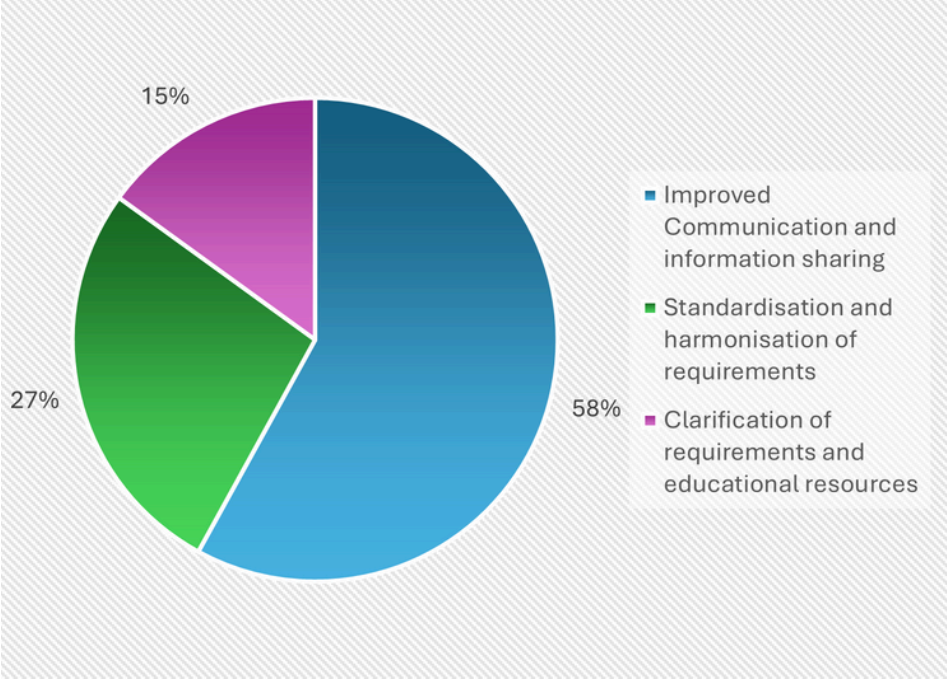


Figure 12 *How to improve collaboration with supervisory authorities?*

Organisations strongly prioritize better communication and information sharing with supervisory authorities, with 58% identifying this as the key area for improvement. Suggestions included regular updates, webinars, Q&A sessions, and dedicated information channels. Many respondents expressed concern about dealing with different requirements in different countries. 27% of suggestions called for more practical guidance, templates, checklists, or concrete implementation steps. 15% of responses indicated a need for clearer definitions of who falls under NIS2 scope as they specifically mentioned difficulty in self-assessing their NIS2 applicability and what exactly is required to be compliant.

IMPLEMENTATION CASE STUDIES

6.

6. Implementation Case Studies

The case study analysis in this paper draws from contributions provided by ECSO members, with particular emphasis on the input from the ECSO CISO Community. While the case studies have been anonymized to protect confidentiality, they offer valuable insights into the varying levels of NIS2 preparedness across different sectors:

- Energy
- Healthcare
- Manufacturing
- Manufacturing of electrical equipment
- ICT Service Management
- Managed Security Provider (MSSP) - 2 case studies
- Finance
- Public administration

6.1. Energy

An energy sector organisation's NIS2 implementation builds upon their existing NIS1 compliance framework, while addressing several organisational challenges to enhance their security posture. Despite having established security measures through sector specific national laws, the company identified key areas needing improvement, particularly in coordination between different security functions.

Initial assessment revealed structural challenges: separated IT and OT security departments with limited synergy, a hybrid SOC model with an external third party, and unclear role definitions between CSIRT, SOC, CISO organisation, and compliance teams. To address these gaps, they formed a comprehensive task force including the CISO, OT Security head, legal and compliance representatives, internal audit, and external consultants.

The implementation strategy focused on maturing and harmonising their security framework, adopting ISO/IEC 27001 as an umbrella framework while mapping to NIST and IEC 62443 standards. Key improvements included enhancing risk management to cover supply chain risks, introducing attack surface modelling, expanding SOC capabilities with threat hunting, and strengthening CSIRT's incident response capabilities. They also focused on maturing crisis management, streamlining incident reporting, and enhancing business continuity measures.

Their experience yielded valuable lessons: the importance of strong communication with senior management regarding liability and responsibility, the need for broad stakeholder involvement from the outset, the value of building upon existing frameworks while streamlining processes, and the benefits of an agile implementation approach.

6.2. Healthcare

Foundation for the NIS2 implementation rests on a robust information management framework that ensures governance through regular C-level and board discussions. Drawing from successful NIS1 audits, they anticipate being already compliant with many provisions of NIS2 but have the plan to verify this with external auditors.

Resource allocation has been carefully considered, with plans to expand beyond the previous 30-40% time commitment of two staff members to meet NIS2's broader requirements. The organisation's cybersecurity framework integrates multiple standards (ISO27k, NIST, COBIT) into practical controls across IT and business operations. Supply chain security, already strengthened through GDPR and GxP compliance, includes comprehensive supplier assessments and OT environment protection.

Their established SOC handles incident reporting, requiring minimal adaptation beyond threshold definition updates. A key focus is maintaining compliance agility as they face multiple incoming regulations (NIS2, CER, ESG, supply chain directives). Information management framework is designed to adapt swiftly to legislative changes, ensuring continuous compliance across evolving requirements.

6.3. Manufacturing

A manufacturing organisation's journey to NIS2 compliance showcases a structured yet adaptable approach, despite having no prior experience with NIS1. At the heart of their implementation is a dual-framework approach merging governance and technical controls. The governance framework establishes 7 core policies and 13 essential controls, supported by regular bi-monthly management meetings. This is strengthened by deep cross-departmental collaboration, bringing together legal, data privacy, compliance, and IT teams to ensure comprehensive coverage of NIS2 requirements. The technical implementation combines ISO 27002 and NIST Cybersecurity frameworks, creating a robust system of 113 controls mapped to NIS2 requirements. By prioritizing 13 high-impact controls, the organisation maintains focus while building a comprehensive security foundation. This hybrid approach maximizes the strengths of both frameworks - ISO 27002's structured security controls and NIST's flexible risk management approach.

Operational execution shows particular attention to supply chain security, implementing thorough vendor assessments and clear contractual requirements, especially for those handling sensitive information. The organisation has also refined their incident response protocols by incorporating NIS2's threshold definitions, ensuring appropriate CERT notifications.

6.4. Manufacturing of Electrical Equipment

A major manufacturer of electrical equipment approaches NIS2 implementation with systematic planning, recognizing its significant impact due to their extensive European operations. The organisation has established a dedicated task force to monitor national transpositions and maintain engagement with cybersecurity authorities.

Additionally, a compliance process is operationalized at company level using a systematic approach. This process begins with the understanding of the obligation by posing key questions like:

- Has my company identified and assessed its cybersecurity risks?
- Is there an appropriate cybersecurity policy framework in place?
- Are employees regularly trained in cybersecurity, including but not limited to incident reporting?

By addressing these questions, the organization aligns requirements with internal initiatives from its cybersecurity roadmap. The structured approach to responding to regulations is guided by the company's cybersecurity policy framework. These policies set rules and expectations to ensure secure behaviours and practices are applied throughout the company. They cover people, technology, and process controls. By mapping each requirement to internal policies, it ensures that NIS2 requirements are addressed within the company, helping to identify owners and any areas needing attention.

The organisation emphasizes collaborative implementation through dedicated workshops that serve multiple purposes: raising awareness about NIS2, preparing implementation processes, conducting gap assessments, and ensuring team readiness for compliance.

6.5. ICT Service Management

Being new to NIS regulatory requirements, their transition benefits from strong executive engagement, with a dedicated committee comprising the General Manager, Compliance Manager, and relevant Business Line Managers overseeing the compliance project.

Their operational readiness is supported by an incident handling process, enhanced by an externally managed MDR service. While they maintain established processes for supply chain security and contractual requirements, the organisation recognises the need to strengthen third-party auditing procedures to better manage associated risks.

Looking forward, the organisation anticipates increased security audits but maintains confidence in their cybersecurity posture and expertise.

6.6. Managed Security Service Provider (1)

MSSP's implementation of NIS2 highlights a unique dual responsibility in the cybersecurity landscape. As an essential entity, they must both ensure their own compliance while simultaneously providing security services and incident reporting support to their clients.

Organisation has adopted an alignment with the NIST framework to address NIS2 requirements systematically. Their comprehensive security approach begins with robust Cyber Threat Intelligence collection and asset mapping through a Configuration Management Database. Protection measures integrate both Red Team vulnerability assessments and Blue Team weakness identification, feeding directly into development processes.

Their detection capabilities focus on advanced Security Operations Centre, combining SIEM for comprehensive log management with SOAR technology for automated response. The incident management structure is particularly noteworthy, making a clear distinction between cyber incidents and cyber crises to align with NIS2's significant incident definitions. This is supported by an internal CSIRT handling both incident response and crisis management.

Particular challenge emerges in cross-border operations, where an MSSP providing services from one country to entities with critical assets across multiple nations faces uncertainty about specific requirements.

6.7. Managed Security Service Provider (2)

Despite not being under NIS1's scope, the organisation's ISO 27001 certification provides a strong foundation, with their existing cybersecurity risk management measures aligning naturally with NIS2 requirements.

Governance structure reflects a mature security posture, with both cybersecurity and risk management embedded in mandatory controls. Leadership is well-structured, with the General Counsel overseeing risk management practices (aligned with stock listing requirements) and the CISO directing cybersecurity initiatives, both serving on the Global Leadership Team. This arrangement is supported by a dedicated legal team handling regulatory compliance.

While their established security practices require minimal adaptation, the organisation recognizes supply chain security as a key focus area requiring enhanced management activities. Their existing relationship with the national CSIRT has fostered strong information exchange practices and voluntary reporting protocols, complemented by established customer notification procedures when necessary.

6.8. Finance

The bank's approach to NIS2 implementation begins by conducting an organisation-wide business impact assessment to identify critical services and processes. This approach becomes particularly efficient because they're already implementing DORA (Digital Operational Resilience Act), allowing them to leverage existing documentation and assessment work rather than starting from scratch. Their implementation benefits from strong organizational foundations. A dedicated compliance team follows a well-defined process covering surveillance, gap analysis, planning, and implementation, while a CEO-established regulations committee provides management oversight. The bank's existing ISO27001 certification further strengthens their position for NIS2 compliance.

The bank views NIS2 not as an operational challenge but primarily as a documentation exercise. Their focus lies in demonstrating compliance and aligning existing processes - such as incident management and supply chain security - with new requirements.

6.9. Public Administration

The organization bases its security framework on both NIST and ISO 27001 standards, though they use these as reference points for best practices rather than strict compliance guidelines.

Their security infrastructure demonstrates both strengths and areas needing development. They conduct regular System Readiness Assessments, their incident response capabilities are well-developed, and they implement security measures including multi-factor authentication, encryption policies, and regular vulnerability assessments with internal audits and monitoring.

A backup restore procedure is described in the relevant policy, testing is done twice per year and a disaster recovery plan linked to standards operating procedures is under development. There is not a crisis management process as an overall process.

Adaption to NIS2's enhanced requirements, particularly around supply chain monitoring and stricter reporting deadlines, remains a work in progress.

Avenue des Arts 46, 1000, Brussels (Belgium)
sebastijan.cutura@ecs-org.eu
www.ecs-org.eu