ECSO
EUROPEAN CYBER SECURITY ORGANISATION

NIS2 Directive Implementation State of Play: National Transposition, Entities Readiness Level, and Sectoral Applications

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

Europe’s Voice in Cybersecurity

The „go-to” association in Europe focusing on cybersecurity

- Created in 2016 as the contractual counterpart to the European Commission for implementing **Europe’s unique Public-Private Partnership in Cybersecurity (2016-2020)**
- The aim of the partnership was to foster **cooperation between public and private actors** in order to allow people in Europe to access innovative and trustworthy European solutions
- Today, ECSO builds upon the many successes of the Partnership and with its cross-sectoral membership base contributes to **developing cybersecurity communities** and builds the **European cybersecurity ecosystem**
- ECSO's diverse membership, encompassing the full spectrum of cybersecurity stakeholders, enables 360-degree coverage of cybersecurity topics

Members

Large companies (users and providers)

SMEs & start-ups

Research centres, universities

European, national and **regional clusters** & **associations**

Local, regional and national **public administrations**

Investors

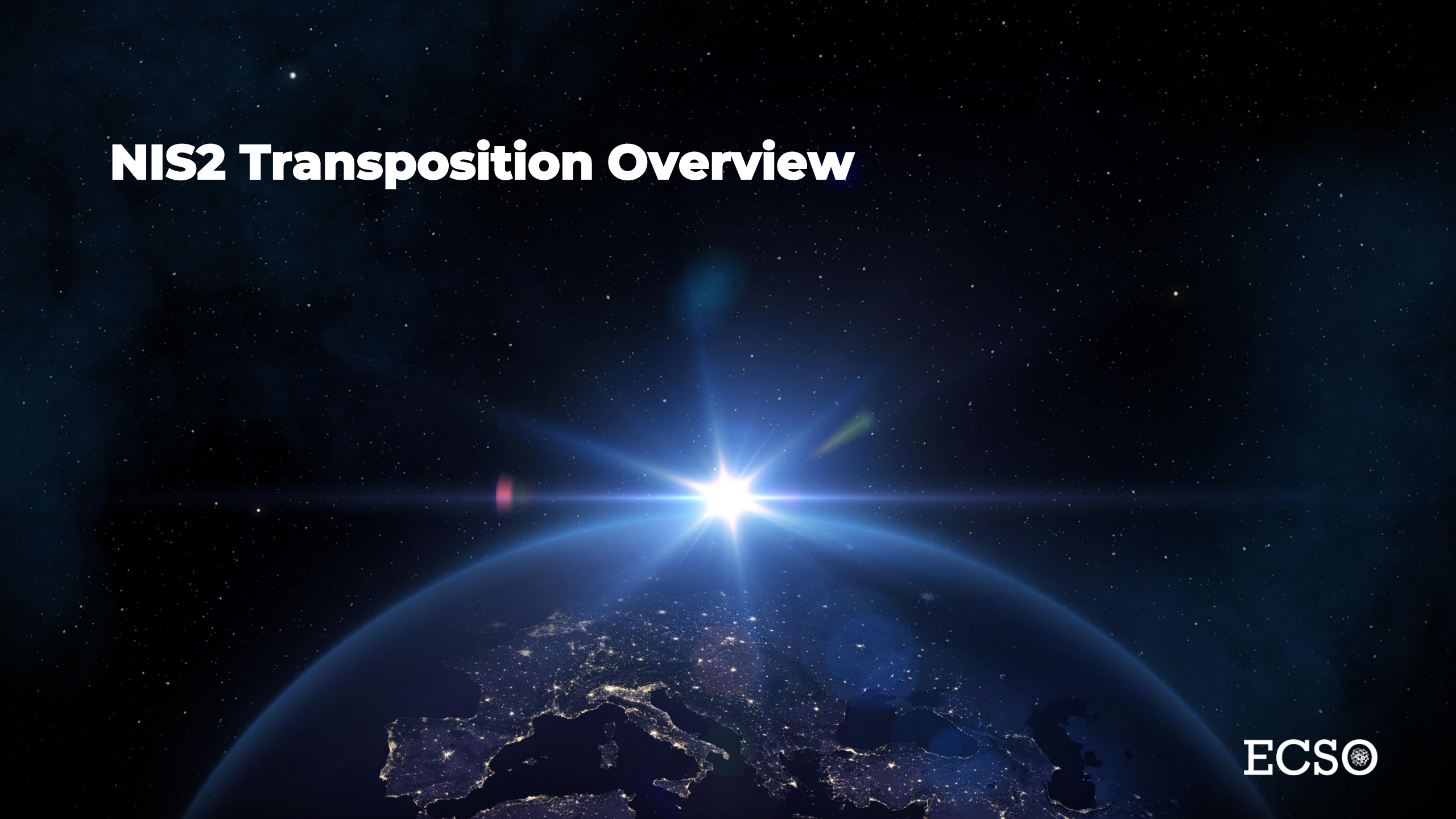
End-users and operators of critical infrastructures and essential services

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

ECSO

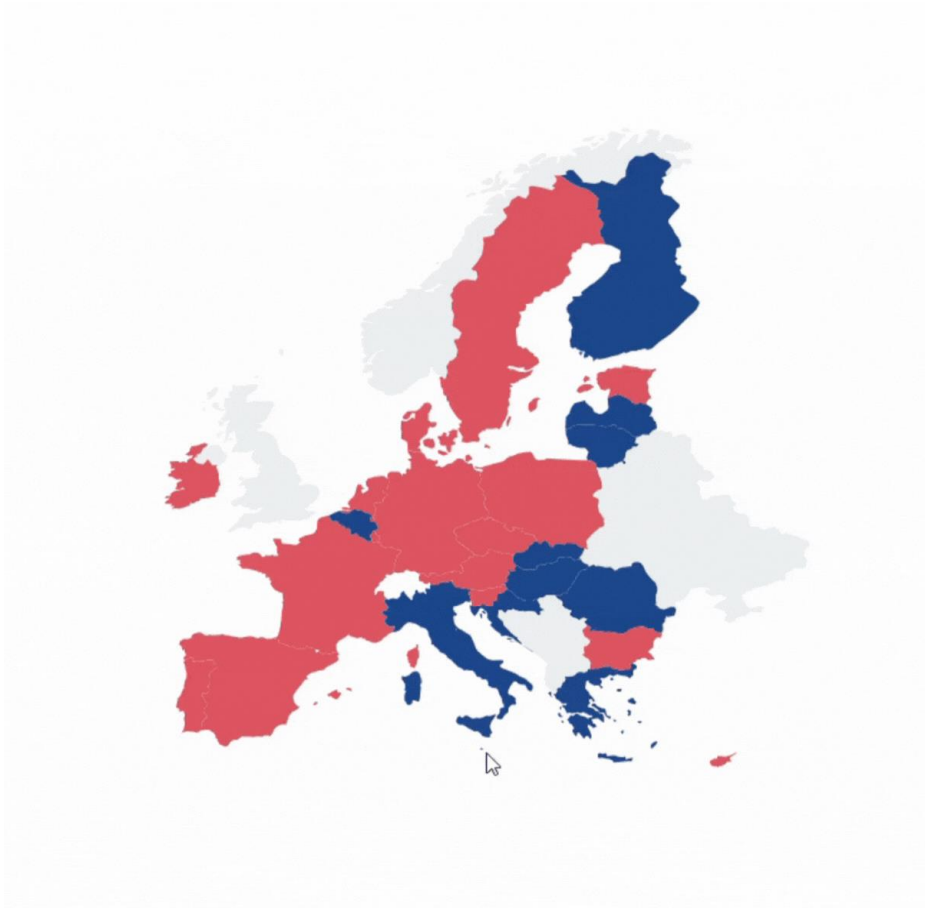
NIS2 Transposition Overview



ECSO

NIS2 First-Hand Challenges

NIS2 Transposition Status



Transposed Draft Law

ECSO's NIS2 Transposition Tracker developed in collaboration with the ECSO CISO Community

Latest Developments

- 11 laws and 16 draft laws
- Croatia, Italy, Belgium, Lithuania, Greece, Romania, Hungary, Slovakia, Finland, Latvia, and Malta are the only countries that fully transposed NIS2
- We expect Denmark to implement the Directive by the end of the summer
- Transposition was postponed due to recent elections, government changes, complex legislative processes or delays in stakeholder consultations

ECSO

NIS2 First-Hand Challenges

Enlarged Scope and Layered Entity Classification

Added intermediaries in the ICT sector, public administration and education

Added mineral extraction and electronic communications as subsectors and all types of manufacturing as one sector under essential entities

Entities fall into 3-tier security levels – security measures depend on the level. Added public transport and manufacturing of cement, lime, and plaster as subsectors

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

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

Introduces the same security obligations for both essential and important entities

Allows certain entities to be excluded if they operate independently from partners and linked companies

Key Takeaway

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

Note: This information is accurate to the best available knowledge as of January 2025.

NIS2 First-Hand Challenges

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

CyberFundamentals Framework based on NIST CSF, ISO 27001/27002, CIS Controls and IEC 62443

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

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

National Framework based on ISO 27001 and NIST 800-53 and recognising Belgium's CyberFundamentals Framework

Key Takeaway

Companies must maintain different documentation sets, security controls, and audit processes to satisfy essentially the same NIS2 requirements across different member states, while also managing the ongoing challenge of standards versions and updates being accepted at different times by different countries.

Note: This information is accurate to the best available knowledge as of January 2025

NIS2 First-Hand Challenges

Timelines Divergences

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

Organisations to be compliant by September 2026

One year after the registration confirmation

18 months after end of the registration period

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

Key Takeaway

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

Note: This information is accurate to the best available knowledge as of January 2025

ECSO

NIS2 First-Hand Challenges

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

Key Takeaway

The divergent scope of reportable incidents across countries, with some requiring reporting beyond significant incidents modifying the timeline, forces companies to implement broader monitoring capabilities and maintain country-specific incident response procedures, leading to increased resource requirements

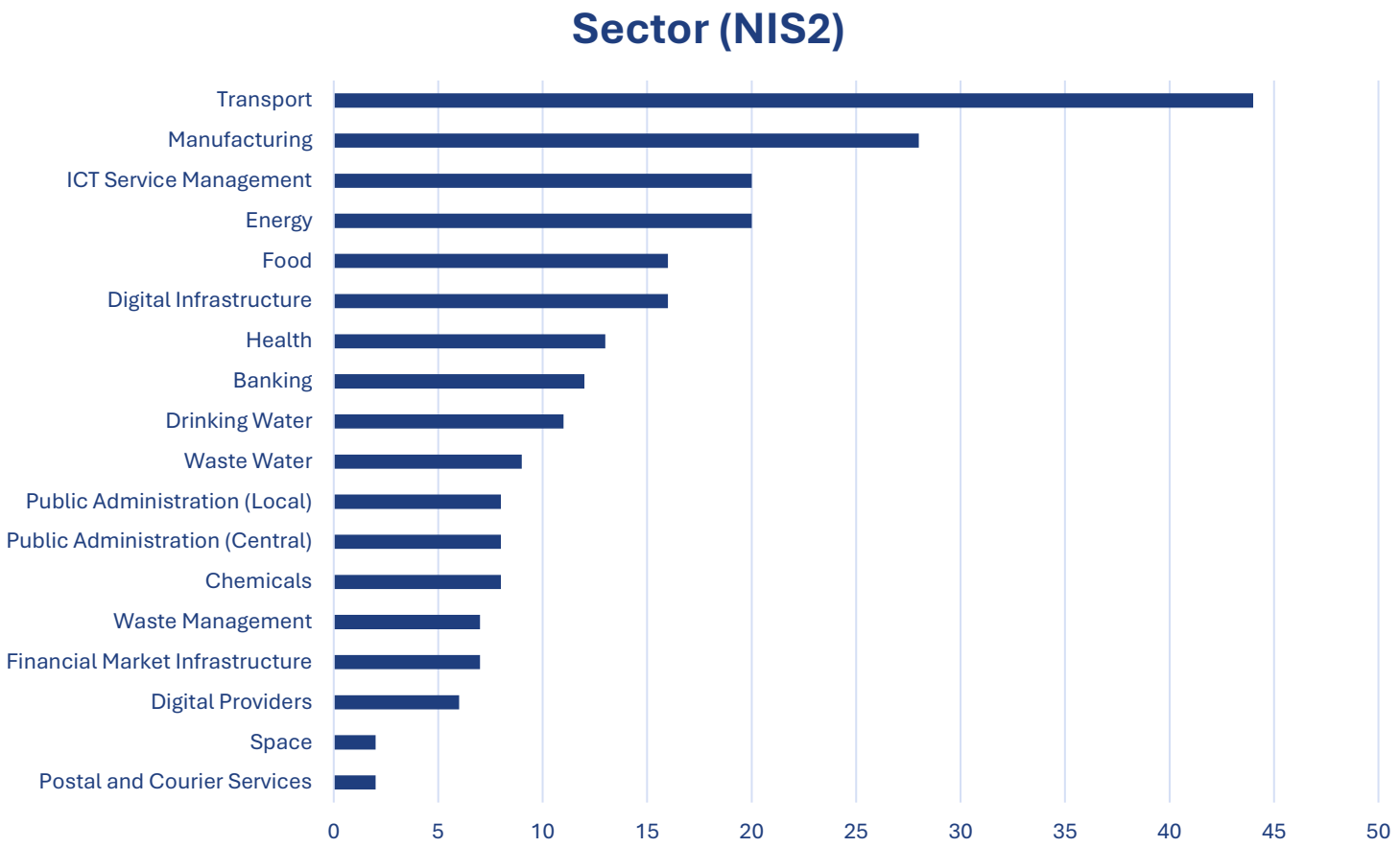
Note: This information is accurate to the best available knowledge as of January 2025

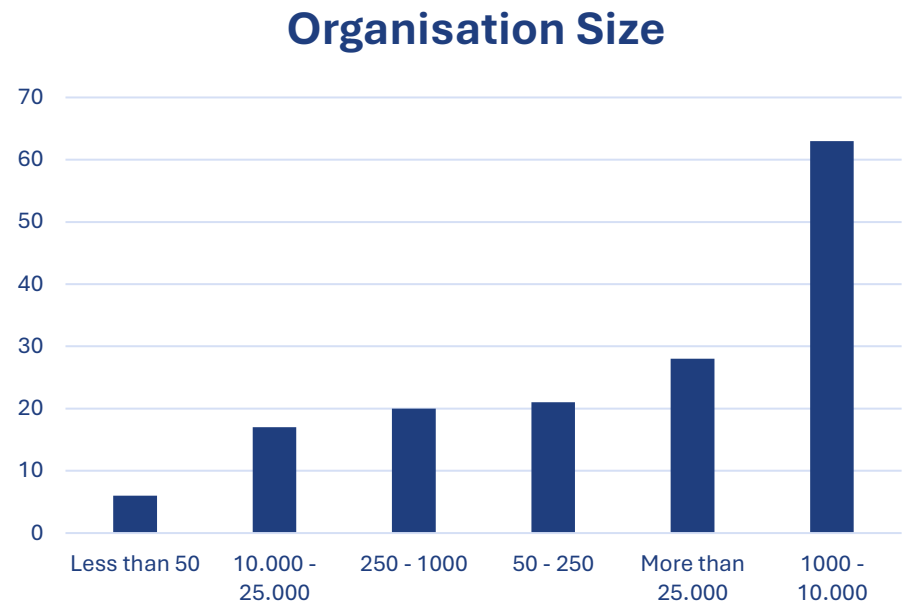
ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Practitioner's Survey

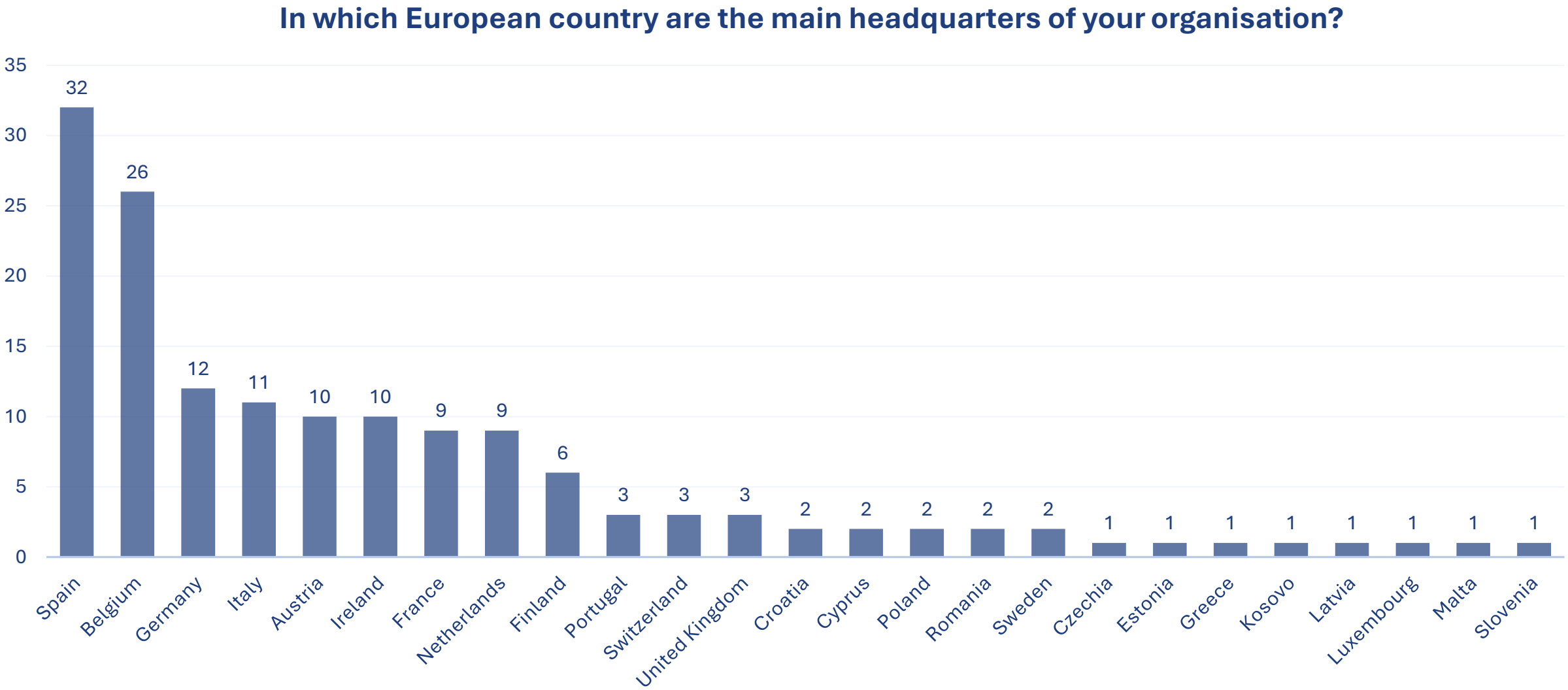
155 responses from 23 European countries

Profiling: NIS2 Sector & Organisation Size



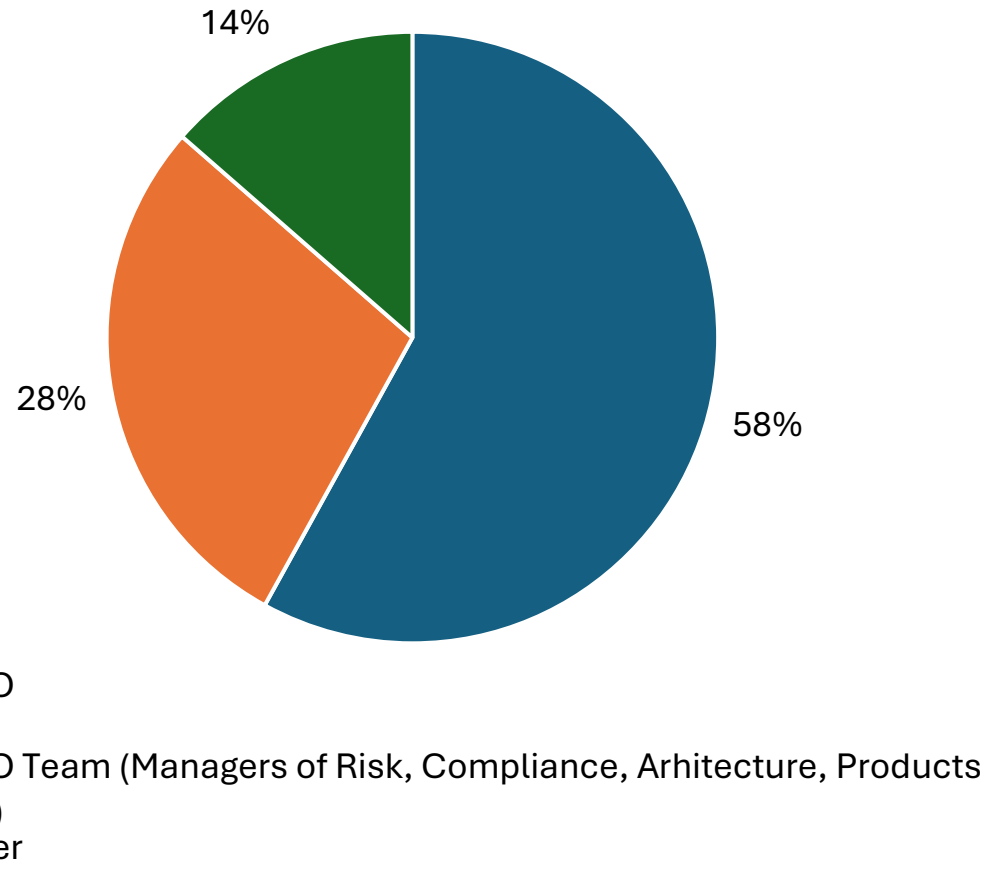


Profiling: European Headquarter

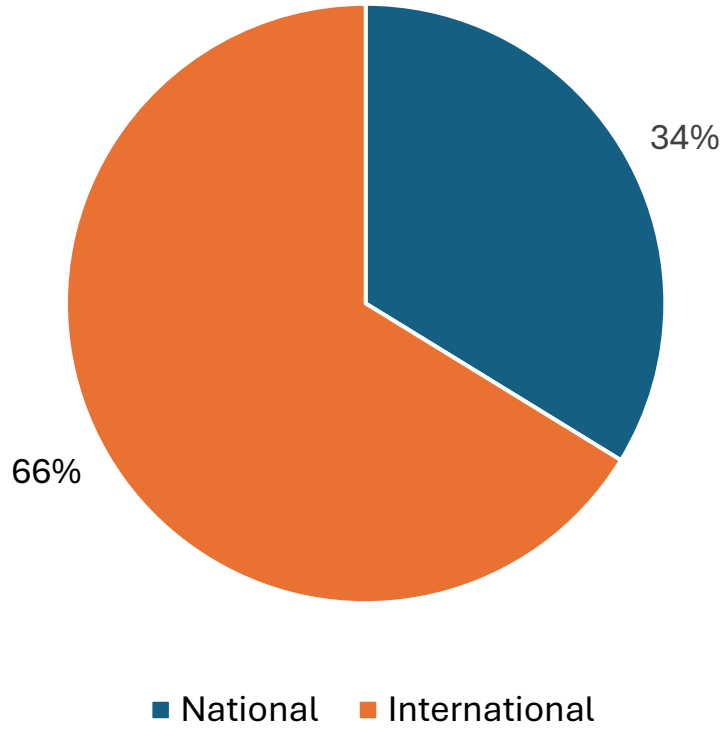


Profiling: Titles and Scope of Operations

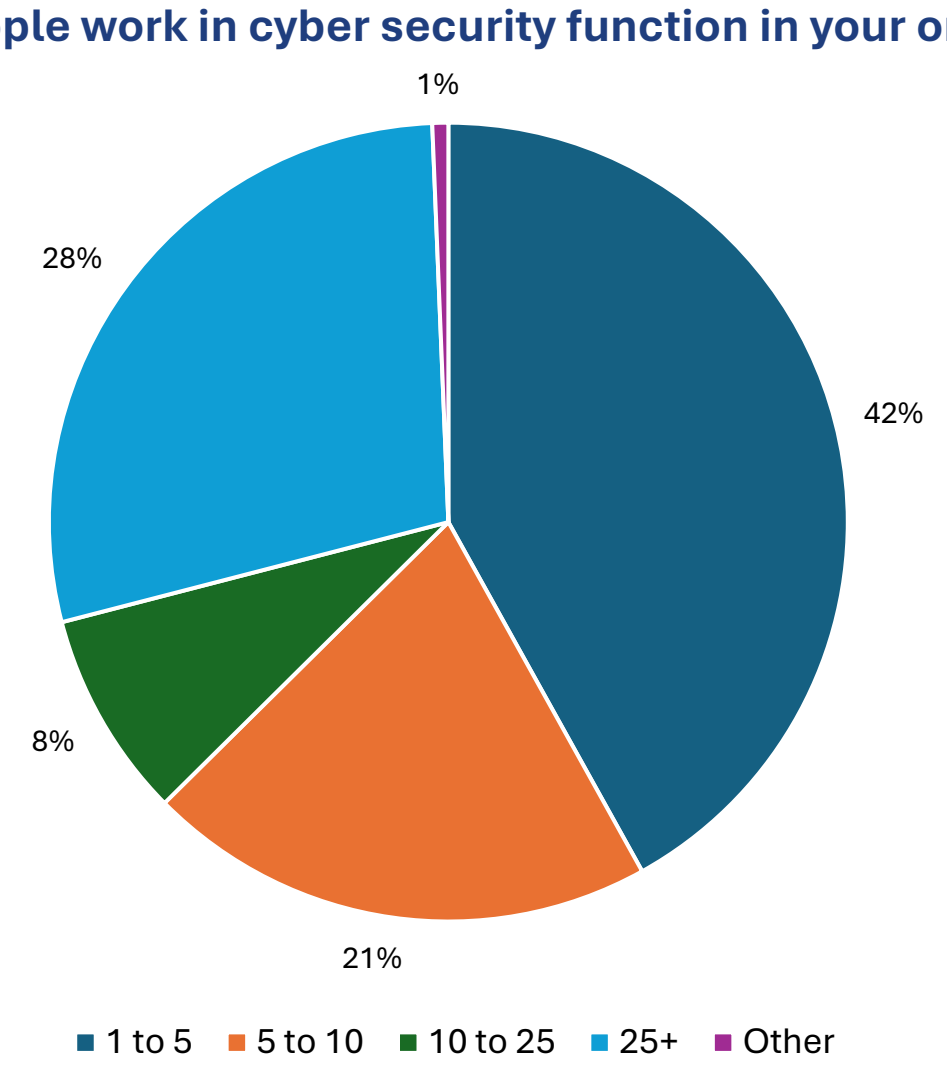
Title of respondents



Are Operations of your Organisation in One Country or International?

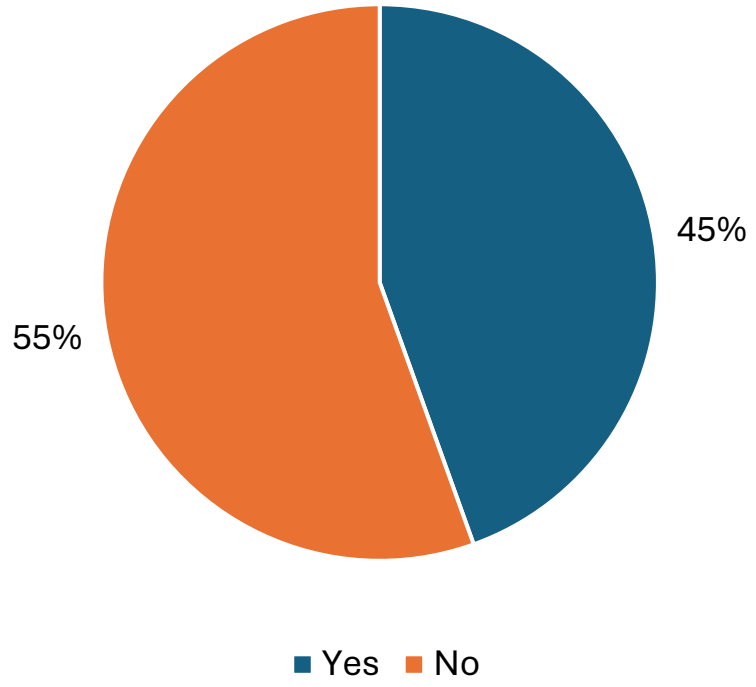


Profiling: Size of Cybersecurity Team

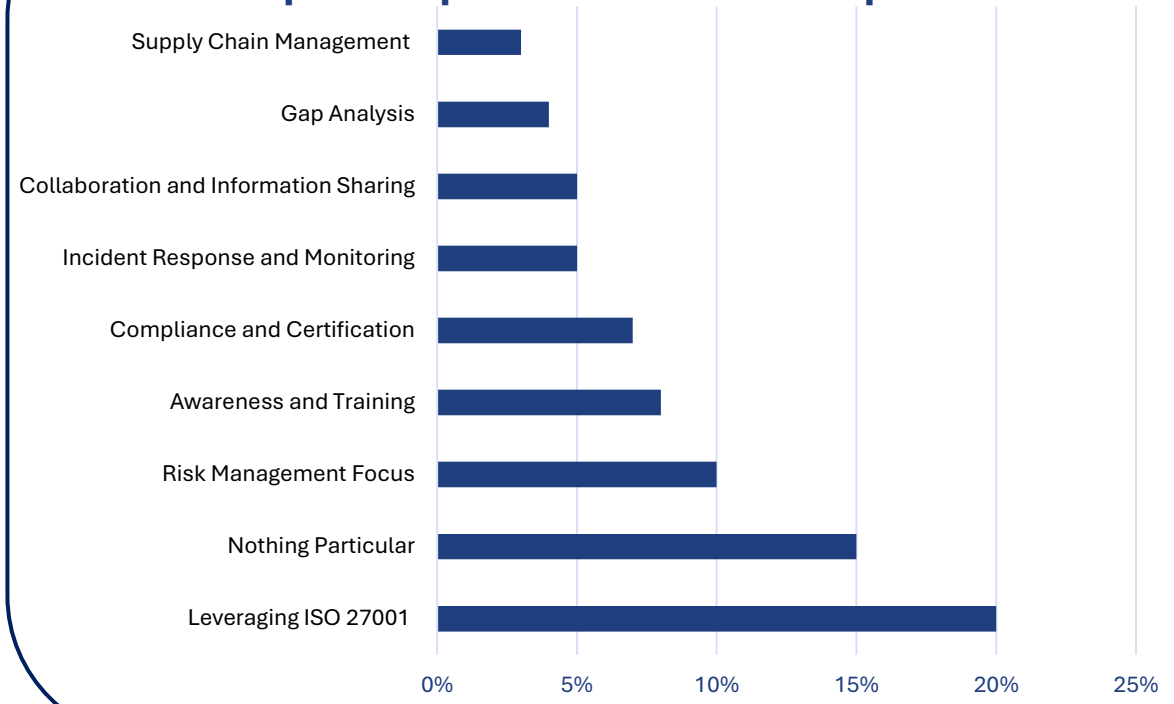


Transition from NIS1 to NIS2

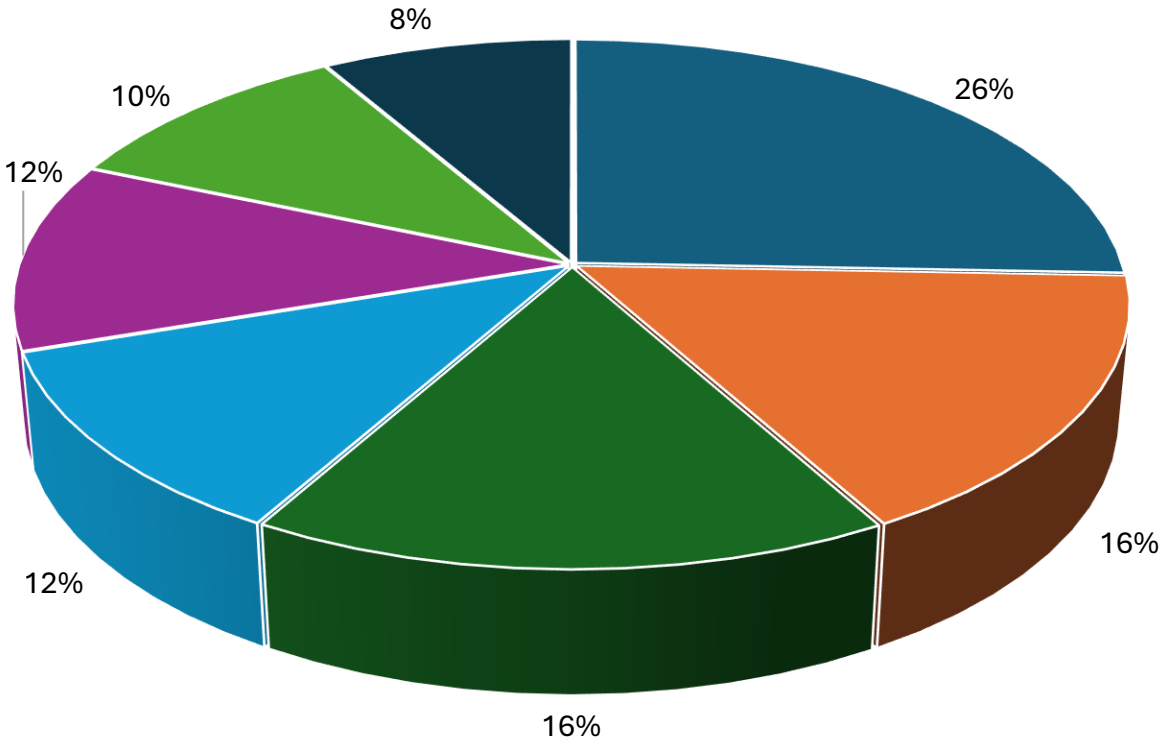
Was your organisation in the scope of the NIS1?



Frequency of mentioned best practices of companies part of the NIS1 scope

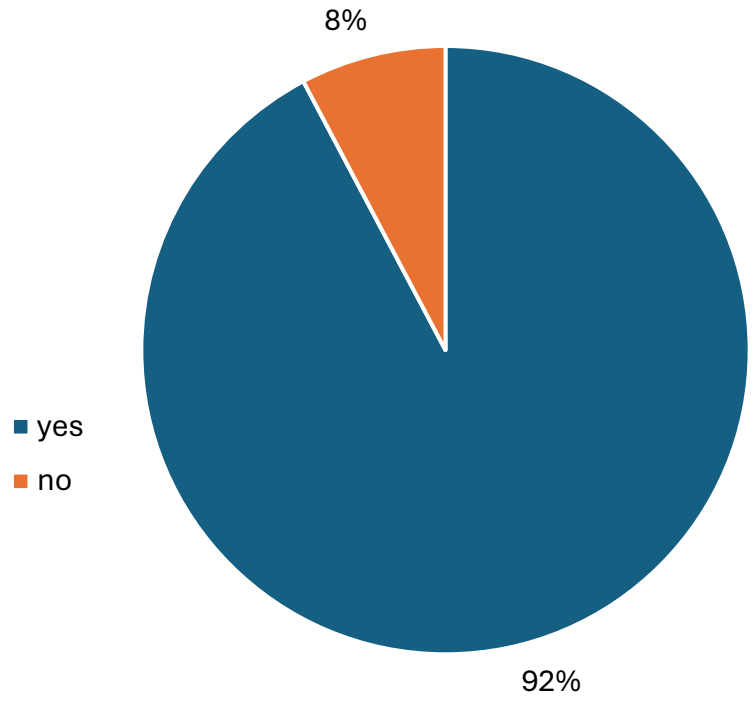


NIS2 Implementation Key Challenges

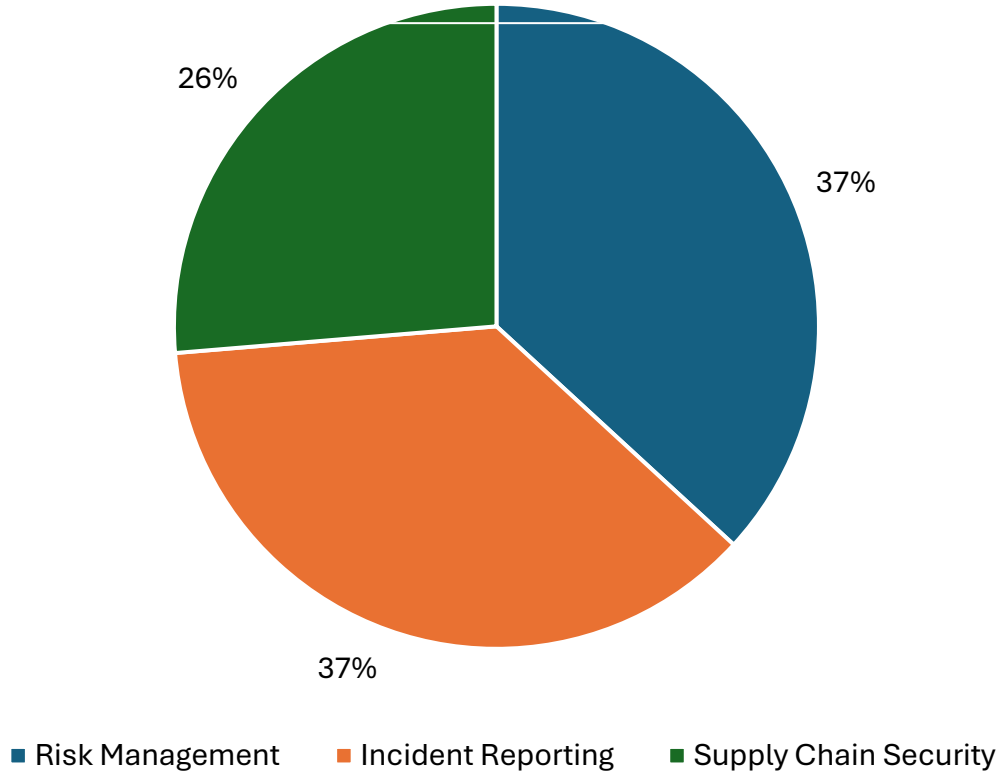


Guidelines and Templates to Facilitate Compliance

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

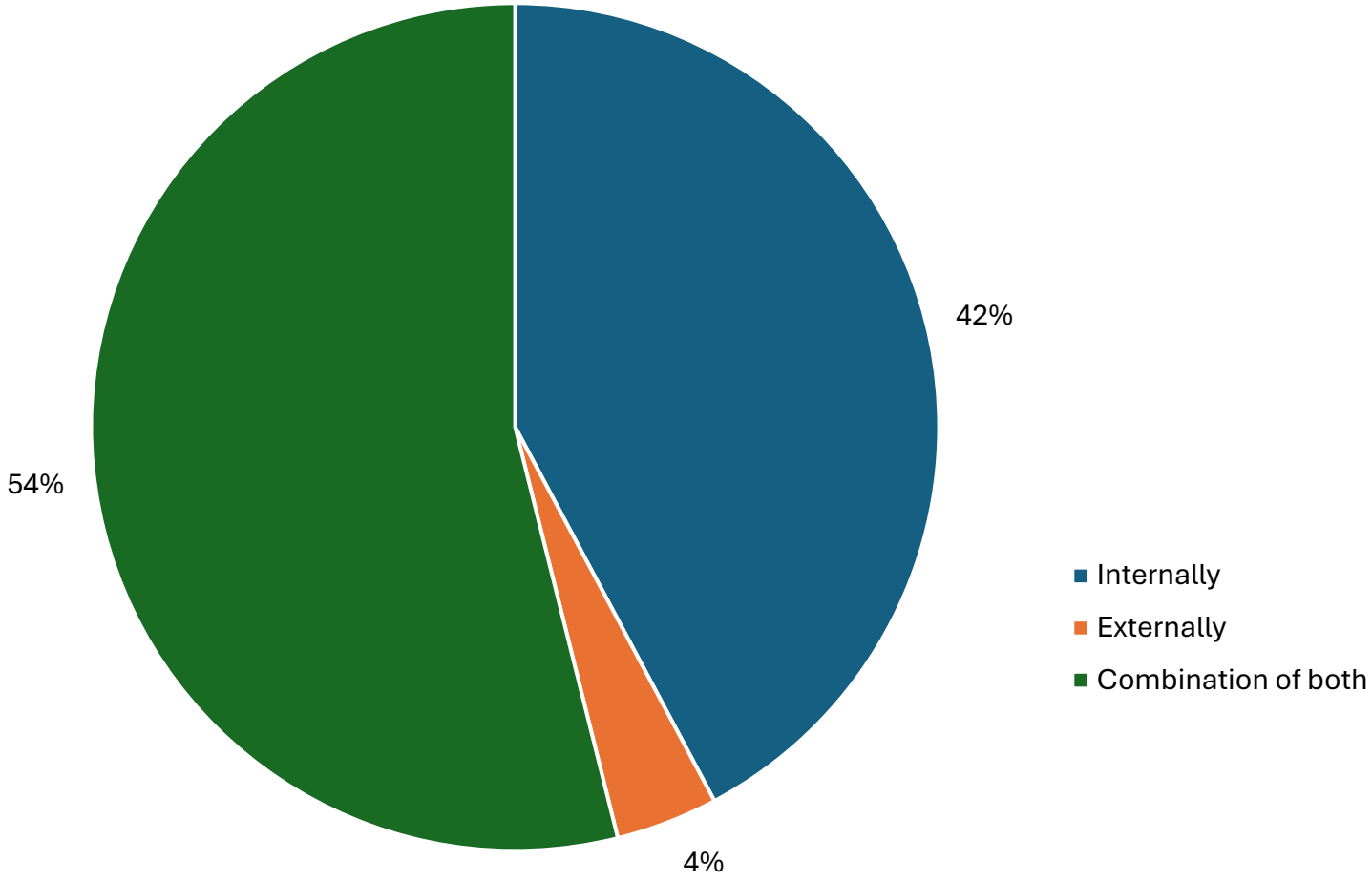


Indicate the type of document and required content that would help you



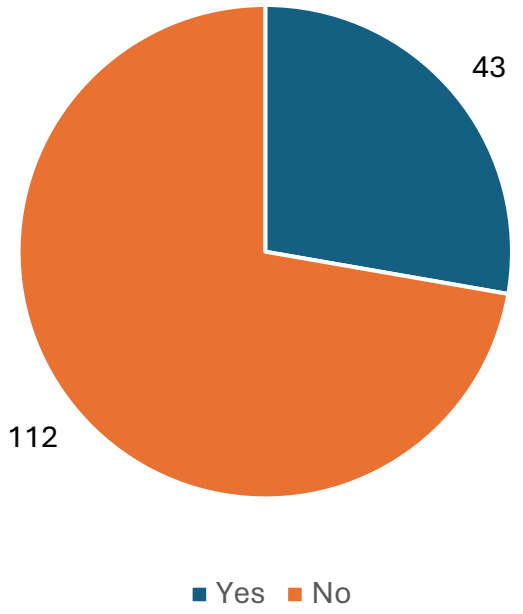
NIS2 Implementation Support

Is the NIS2 Implementation in your organisation conducted internally or with the support of external organisations?

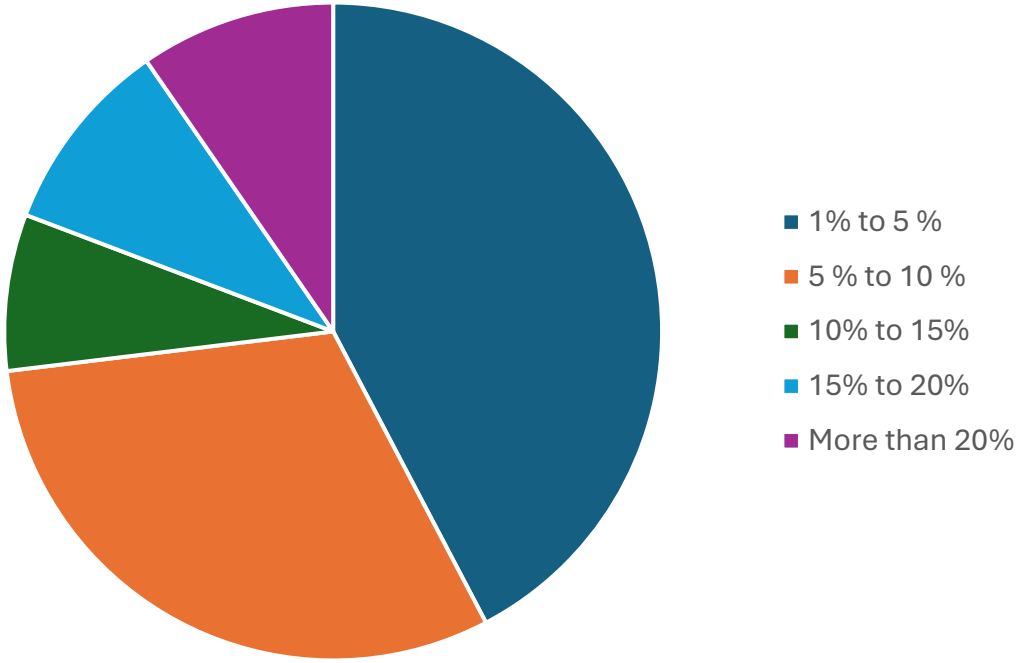


NIS2 Implementation Budget

Do you have a dedicated budget for the NIS2 Implementation?

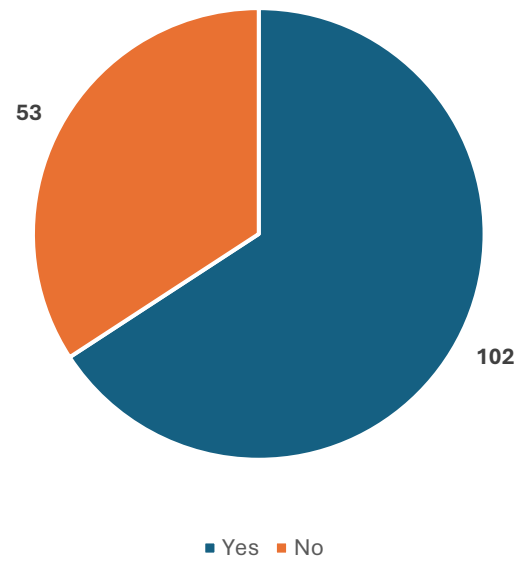


If yes, could you please indicate the financial value reserved for the NIS2 (as % of the total cybersecurity budget)?

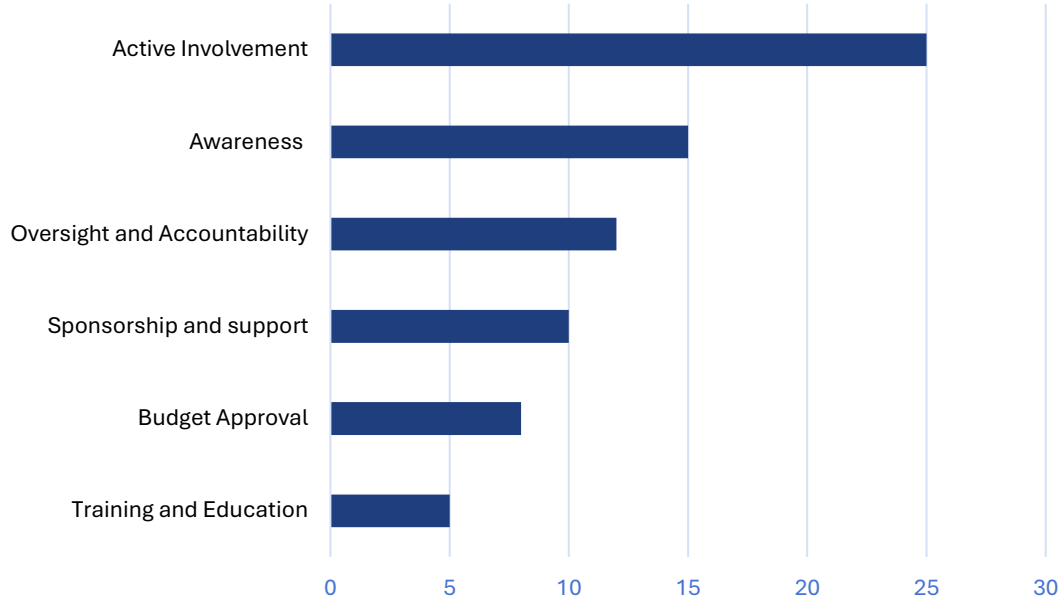


Involvement of Top Management

Is the top management involved in the NIS2 Implementation?



If yes, could you elaborate on how the top management is involved?



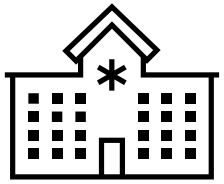
ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Sectoral NIS2 Implementation Case Studies

Implementation Case Studies – Energy, Healthcare and Food Manufacturing

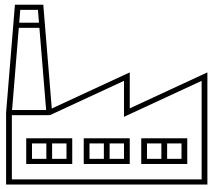
Energy

Regulatory Context: Building upon existing NIS1 framework and sector-specific requirements
Key Challenge: IT/OT Gap, Hybrid SOC with external third party, unclear role definition between CSIRT, SOC, CISO and compliance teams
Unique Approach: Adopting ISO 27001 as umbrella framework while mapping to NIST and IEC 62443 standards. Enhancing risk management to cover supply chain risks, expanding SOC capabilities and strengthening CSIRTs incident response capabilities



Healthcare

Regulatory Context: Leveraging on NIS1 audits anticipating being already compliant with many provisions
Key Challenge: Maintaining compliance agility as they face multiple incoming regulations (NIS2, CER, ESG, supply chain directives).
Unique Approach: 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.



Food Manufacturing

Regulatory Context: No prior experience with NIS1
Key Challenge: Particular attention to supply chain security implementing thorough vendor assessments and clear contractual requirements
Unique Approach: Adopting a hybrid approach combining ISO 27002 and NIST Cybersecurity Frameworks and emphasis on adapting incident response protocols to include NIS2 threshold definitions

Implementation Case Studies – Manufacturing, ICT Services, MSSP

Manufacturing Electrical Equipment

Regulatory Context: Multinational company dealing with varying national NIS2 implementations
Key Challenge: 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?
Unique Approach: 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

ICT Services

Regulatory Context: Provider of critical ICT services, newly in scope for NIS2
Key Challenge: Recognises the need to strengthen third-party auditing procedures to better manage associated risks.
Unique Approach: Operational readiness is supported by an incident handling process, enhanced by an externally managed MDR service and a dedicated implementation committee.

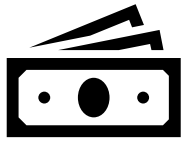
Managed Security Service Provider

Regulatory Context: Essential entity under NIS2
Key Challenge: Balancing own compliance with supporting clients' NIS2 efforts. 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.
Unique Approach: Aligning NIS2 requirements with NIST framework phases for operational integration

Implementation Case Studies – MSSP, Finance, Public Administration

Managed Security Service Provider

Regulatory Context: Essential entity under NIS2
Key Challenge: Recognizes supply chain security as a key focus area requiring enhanced management activities.
Unique Approach: Leveraging ISO 27001 with existing cybersecurity risk management measures



Finance

Regulatory Context: Heavily regulated industry, subject to DORA and other financial regulations
Key Challenge: The bank views NIS2 not as an operational challenge but primarily as a documentation exercise.
Unique Approach: Leveraging existing Business Impact Assessment from DORA implementation

Public Administration

Regulatory Context: Essential entity under NIS2, subject to public sector regulations
Key Challenge: Adaption to NIS2's enhanced requirements, particularly around supply chain monitoring and stricter reporting deadlines
Unique Approach: Using a "hybrid" combination of NIST and ISO 27001 controls

Nine Recommendations

1. Designate **one single point for reporting of ALL cybersecurity incidents**, beyond the NIS2 scope.
2. **Standardise templates and data formats**, especially focusing **on incident reporting,** with clear definitions to facilitate international communication & problem solving.
3. Develop a **European risk management framework, methodology, and open-source tool**, commonly adopted across EU countries.
4. Develop a **Harmonised EU Supply Chain Security Framework**
5. Rely on **existing standards as a sufficient proof of compliance**.
6. Provide **targeted support for disadvantaged entities** (e.g., timelines, financial incentives for implementation).
7. Create an interactive table **mapping NIS2 security measures to international standards (e.g., ISO, NIST).**
8. Establish a **centralised European information hub** providing an overview of NIS2 transposition status and highlighting key differences across countries.
9. 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 .

Download our Latest Publications

White Paper on NIS2 Implementation

Streamlining Regulatory Obligations

NIS2 Directive Transposition Tracker

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Thank you!

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