ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Streamlining Regulatory Obligations of EU Cybersecurity Policies

10 December 2024

Joanna Świątkowska

European Cyber Security Organisation (ECSO)

Deputy Secretary General

ECSO

Agenda

- Setting the Stage
- Incident Reporting Complexities
- NIS2 First-Hand Challenges
- CRA First-Hand Challenges

ECSO

Research and Analysis Presentation

Cristian Tracci, ECSO
Senior Manager, Policy Analysis and Outreach

Sebastijan Cutura, ECSO
Senior Manager, Industry Cybersecurity

Matteo Mole, ECSO
Manager for Cybersecurity Technologies and Innovation

ECSO

Setting the Stage

How to Streamline Regulatory Obligations?

The Starting Point

The cybersecurity ecosystem is diverse for **size** and **sectoral specificities**.

Cybersecurity policy today does **not fully reflect these differences.**

Policies touch so many different aspects of an organization.

Entities face very **concrete operational challenges** when trying to comply with the existing and upcoming regulations.

The Question

What should be done about it?
Is the solution operational or political?

ECSO

Challenges with Policies and Security Measures

Entities highlighted **challenges** in
almost every domain of cybersecurity,
with variations based on their maturity level, geographical location, and positioning in the market.

First-hand Insights from Security Professionals - Responses from our Survey

Insights from Security Professionals

Quotes from our Survey

*"**Different security and risk mgmt. measures in each country** make central administration **unnecessarily complex**.*
*This complexity **hinders efficient mgmt. and increases operational costs**."*

*"Each regulation prescribes its **own set of security controls** instead of openly requiring established standards.*
*This **inconsistency complicates compliance** efforts and increases administrative burdens."*

*"Implementing CER and NIS2 as **directives rather than regulations** allows each EU country to add its own **variations**.*
*If CER and NIS2 were implemented as regulations, similar to GDPR, it would **reduce uncertainties** and headaches by providing a uniform approach."*

*"Creating customer evidence for compliance is challenging when **requirements are vague**.*
*Understanding regulation priorities when **multiple regulations** affect the solution, and working with authorities in several countries adds **complexity**."*

Note: The opinions expressed in the survey do not represent ECSO official position

The Most Burdensome Requirements

From our Survey

The most challenging areas to comply with include

- **Security requirements harmonization,**
- Risk analysis,
- Data classification and endpoint management,
- **Vulnerability management**,
- Continuous monitoring,
- **Duplicative reporting towards national authorities,**
- **Supply chain** and **security questionnaires**, and
- **Heavy compliance procedures,** including **audits and certifications.**

Note: The opinions expressed in the survey do not represent ECSO official position

Setting the Stage

Access Management

Quotes from our Survey

*"As an international company, we follow both the ISO 27001 and NIST frameworks. However, **password requirements differ between these frameworks**, creating compliance challenges."*

*"NIS2 EU requirements, such as **Multi-Factor Authentication (MFA), differ significantly** from the technical requirements in the **Austrian** NIS2 draft, as well as from those in **Germany** and **Hungary**. This inconsistency complicates compliance efforts."*

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- Today there is a burdensome multitude of legislative requirements and frameworks. **Despite general alignment, there are divergencies on specific details**, which can generate significant operational implications and costs.
- **Mapping domains between different policies and frameworks does not provide a guarantee that specific details align**.

ECSO

Vulnerability Mgmt. and Penetration Testing

Quotes from our Survey

*"**Managing vulnerabilities** to obtain compliance is an ongoing, **energy-draining, and cost-ineffective effort**.*

***Penetration testing** often incurs **significant expenses** and efforts that are perceived as largely unproductive."*

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- While **vulnerability management and penetration testing** is highly **valued security measure.** Some organizations find them overwhelming and may **rather not be required** to perform them.
- Initiatives like **SBOM** and **VEX**, for vulnerability management, and **free scanning services** provided by national cybersecurity authorities, can significantly support smaller entities.

SBOM: Software Bills of Material; VEX: Vulnerability Exploitability eXchange

External Audits

Quotes from our Survey

"Our company is required to prove the level of security to external auditors who are unfamiliar with our operations and rely on a one-size-fits-all checklist.

*These auditors often **charge high rates without enhancing our actual security level**. This process wastes resources that are already scarce in the industry."*

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- Some organizations find the process of proving security levels to external auditors burdensome, as they rely on standardized checklists and don't account for the unique aspects of each organization.
- While some may advocate for more liberalization, the European cybersecurity industry may want to **explore more effective auditing practices**, focused on **security practices rather than formalization.**

Focus Areas

Incident Reporting Complexities

NIS2 First-Hand Challenges

CRA First-Hand Challenges

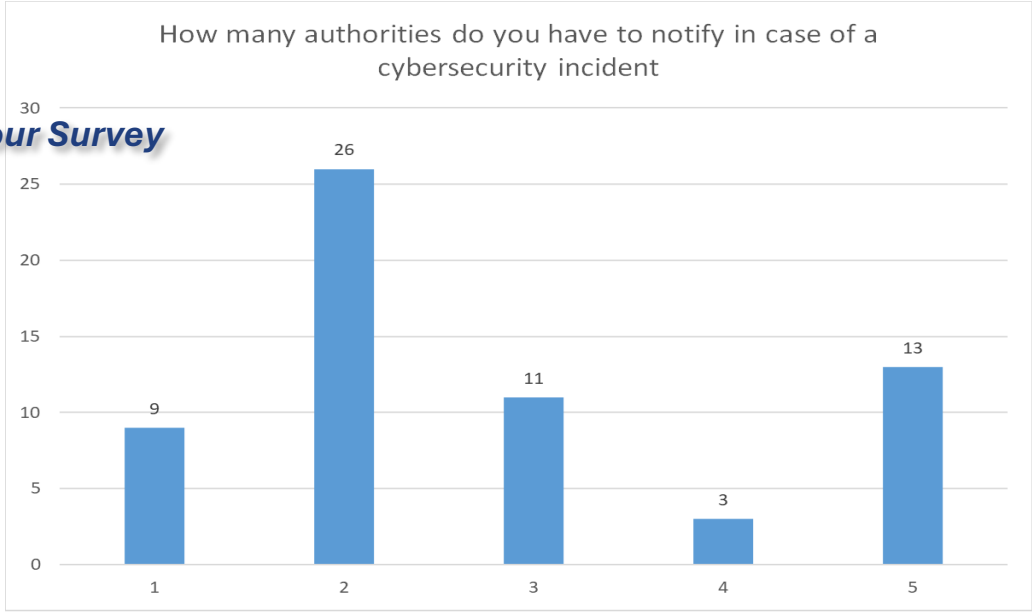
Incident Reporting Complexities

ECSO

Reporting Overview

Notifying incidents to multiple authorities is a major source of complexity, mentioned by multiple respondents.
Financial institutions have the most bodies to notify in case of an incident.
Customers are also to be notified and supported in their notification.

From our Survey



Note: The opinions expressed in the survey do not represent the official position of ECSO or the Kosciuszko Institute

Detailed Desk Research and Analysis

- **NIS2 Directive**
- **Digital Operational Resilience Act (DORA)**
- **Cyber Resilience Act (CRA)**
- **General Data Protection Regulation (GDPR)**
- **Critical Entities Resilience (CER) Directive**

Insights from Security Professionals on Reporting

Quotes from our Survey

*"**As an MSSP provider**, we are both the protector and the protected entity under NIS2 reporting obligations. This may lead to duplicity in reporting incidents. It is unclear **whether a single incident affecting both the MSSP and the service user (critical infrastructure operator) should be reported by the MSSP, the user, or both**."*

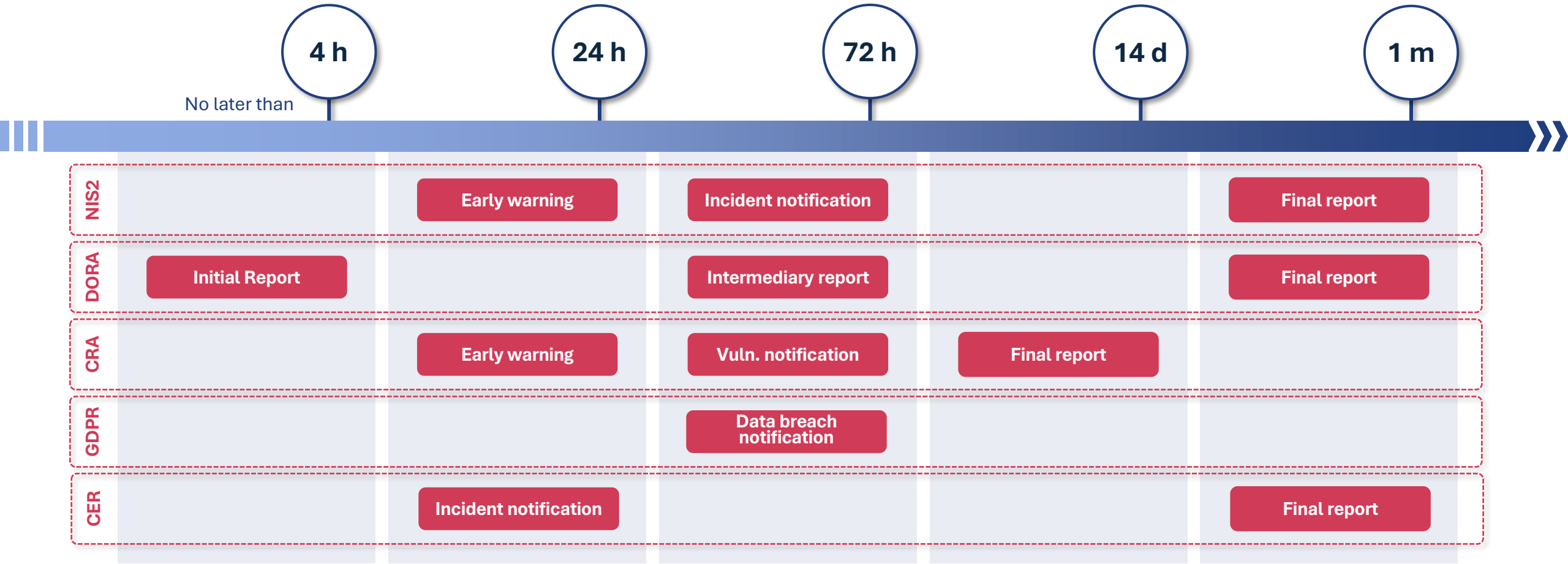
"The answer to this question will not give a picture of our company situation, as under some regimes, we are not the direct subject to reporting but our customers are.
*Our company will need to **assist the customers in assurance of their compliance in their reporting obligations**, by providing all the necessary information in our possession. 5 regimes are in place already and will or may be in place with an impact on our company: GDPR, NIS2, DORA, CRA and AI Act."*

Note: The opinions expressed in the survey do not represent the official position of ECSO or the Kosciuszko Institute

Incident Reporting Complexities

When to Report

Illustrative



Note: This information, collected via interviews, is accurate to the best available knowledge as of November 2024.

ECSO

Incident Reporting in the Finance Sector

CASE STUDY

Up to 20 bodies to notify in case of an incident + national CSIRTs from NIS2 (27 countries)
Potential solution → Financial Supervisory Board - **Format for Incident Reporting Exchange (FIRE)**
FIRE aims to create a standardized format for cyber incident reporting across the financial sector

Financial Entity facing an incident in a given European country

- **EU Financial Supervisory Authorities**
- **National Financial Supervisory authorities**
- **Data Protection Authorities**
- **Cybersecurity Authorities**
- **Sectoral and Specialized Authorities**
- **Law Enforcement**
- **Stock Exchange Regulators**

Types of entities

Belgium: Notification Authorities for Finance

Illustrative

DORA Single Report (to NBB/FSMA) Cascades to: ECB (for significant banks), ESAs (EBA/ESMA/EIOPA),Payment Systems Supervisors

Sectoral and Specialized Authorities

- **National Payment Systems Supervisors for PSD2 (National Bank of Belgium)**
- **Market Infrastructure Regulators for clearing/settlement incidents (National Bank of Belgium and FSMA for market infra supervision)**
- National Security Authorities if classified information involved (VSSE)
- Financial Intelligence Units if money laundering implications (CTIF-CFI)
- eIDAS Supervisory Bodies if trust services are affected (FPS Economy)

EU Financial Supervisory Authorities

- **European Central Bank – for significant banks under SSM**
- **European Banking Authority**
- **European Securities and Markets Authority (ESMA) - for securities-related incidents**
- **European Insurance and Occupational Pensions Authority (EIOPA) - for insurance-related incidents**

National Financial Supervisory authorities

- **National Central Banks of each member state (National Bank of Belgium)**
- **National Financial Supervisory Authorities (FSMA -The Financial Services and Markets Authority)**

Data Protection Authorities

- Lead Supervisory Authority under GDPR (Belgian Data Protection Authority)
- National Data Protection Authorities in affected member states (potentially 27 countries)
- European Data Protection Board (EDPB) for cross-border incidents

Cybersecurity Authorities

- National CSIRT (CERT.be)
- CSRITs/CERTs of affected member states (potentially 27 countries)

Law Enforcement

- National Police Cybercrime Units (FCCU - Federal Computer Crime Unit)
- Europol in cases of cross-border cybercrime

Stock Exchange Regulators

- Relevant Stock Exchange Authorities if listed (Euronext Brussels)
- **Market Supervisory Authorities for market-sensitive incidents (FSMA)**

Note: This information, collected via interviews, is accurate to the best available knowledge as of November 2024.
Bolded Authorities are covered by the DORA Single Report

ECSO

NIS2 First-Hand Challenges

ECSO

NIS2 Challenges: Differences and Complexity

The Directive based approach means companies must navigate **varying national interpretations and implementation timelines across member states**.

Organisations must adapt to inconsistent scope interpretations, security frameworks, varying reporting thresholds and differences in supply chain provisions, creating **operational complexity in cross-border security management and compliance monitoring**.

Scope

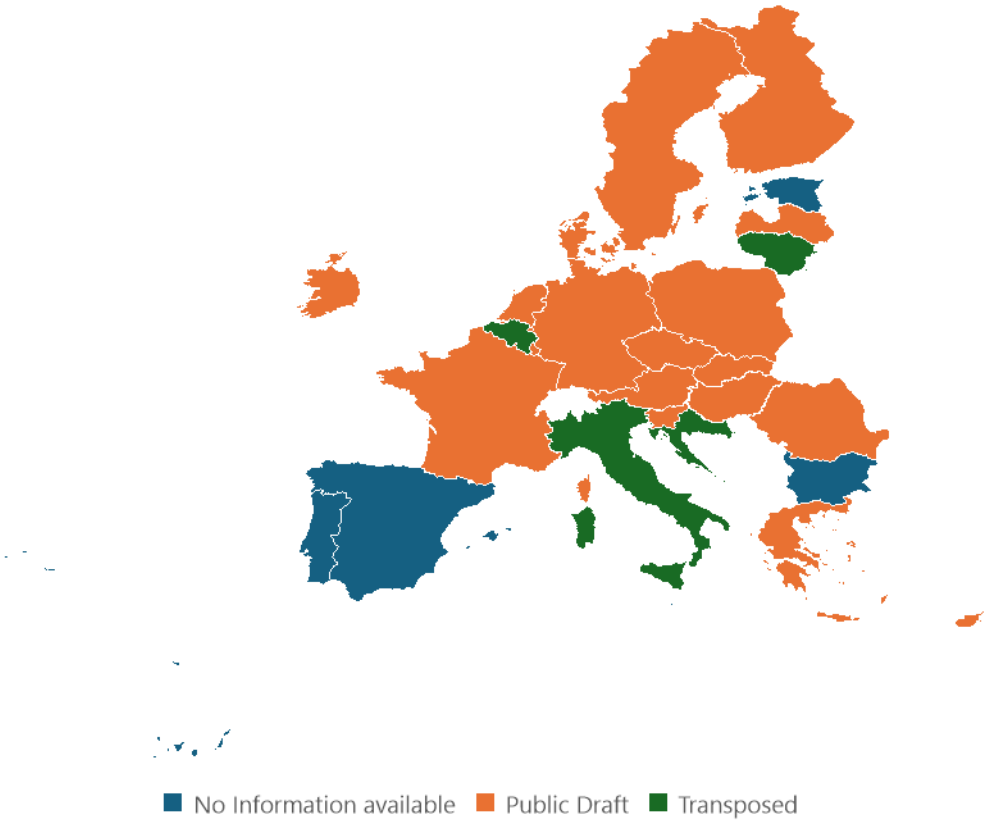
International Security Frameworks

Timeline

Incident Reporting

Supply Chain

Tracking NIS2 Adoption: Latest Developments



Analysis

- Croatia, Italy, Belgium, and Lithuania are the only countries that fully transposed NIS2 based on the infringement procedure started by the EC on 28 November against 23 EU Member States.
- A large number of countries that published drafts expect to adopt NIS2 in Q1 2025.
- 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.

ECSO

NIS2 First-Hand Challenges

Enlarged Scope and Layered Entity Classification

Added intermediaries in the ICT sector, public administration and education

Added mineral extraction, fuel, electronic communications. Manufacturing, production and distribution of chemicals, food production, processing and distribution added to essential entities

Entities fall into three 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 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

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

Omitted the banking and financial market sectors from their national laws

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 November 2024.

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 and the original NIS CG	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	ISO 27001 and NIST 800-53

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 November 2024.

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

8 months after law takes effect

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 November 2024.

NIS2 First-Hand Challenges

Stricter Entity Obligations for Incident Reporting

Requires an early warning within 6 hours of incident detection

Differentiates two types of incidents based on cross-border impact

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 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

Note: This information is accurate to the best available knowledge as of November 2024.

NIS2 First-Hand Challenges

The Hidden Cost of Security Questionnaires

Key Challenges

- **Questionnaire overload (150-1000+ questions)**
- Multiple platforms for questionnaires
- Resource drain (e.g., time, financial resources, and staff)
- Repetitive and time-consuming questions
- Legally binding answers
- New requirements (e.g., AI, ESG) adding complexity
- Concerns about sharing of sensitive documents

Key Solutions

- Minimum European Security Requirements
- Standardized Framework aligned with: NIS2, CRA, ISO, SOC2
- Automated evidence mapping to multiple frameworks and AI assisted pre-filling (75% Pre-filled Common Questions)

Key Takeaway

Standardization can allow to move from checkbox compliance to meaningful security measures.
A minimum-security baseline can be standardized such as in similar examples like CSA's Cloud Controls Matrix (Cloud)* or Minimum Viable Secure Product (Products)*

* The examples suggested here do not represent ECSO official endorsement

CRA First-Hand Challenges

ECSO

Insights from Security Professionals on the CRA

Quotes from our Survey

Supply chain compliance with CRA

"Most of our life science tools contain digital elements sourced from supply chains. Additionally, providing support for up to 10 years for all our products will cause a major cost impact and could potentially kill our business."

Conformity Assessment Processes differences between CRA and EUCC

"CRA allows for internal conformity assessment for class I products if European certifications are used, while EUCC requires third-party conformity assessment as the default regime. This discrepancy adds to the complexity of compliance."

Accreditation Schemes differences between NESAS/CRA

"Accreditation schemes for laboratories vary between NESAS/CRA, leading to compliance risks and potential invalidation of certifications."

Note: The opinions expressed in the survey do not represent ECSO official position

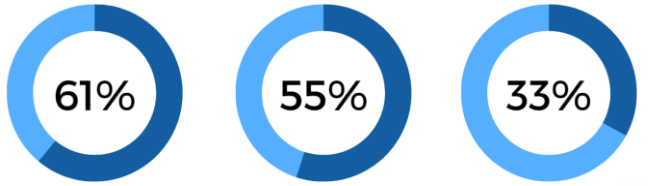
Recurring CRA Implementation Challenges

ECSO has conducted **analysis** on an ongoing basis,
concerning the **perceived challenges and outstanding questions** on the CRA implementation.
Consulting with members, partners organisations, and institutions **some themes are recurring**.

Challenges

- **Product Categories**
- **Proposed Timeline**
- **Clarity of procedure for risk assessment and for conformity assessment**
- **Availability of Standards**

Based on the EC initial CRA proposal



At least one product falling under "Class 2"

At least one product falling under "Class 1"

have product in all classes (including default)

Many respondents estimate a cost increase of **18%**

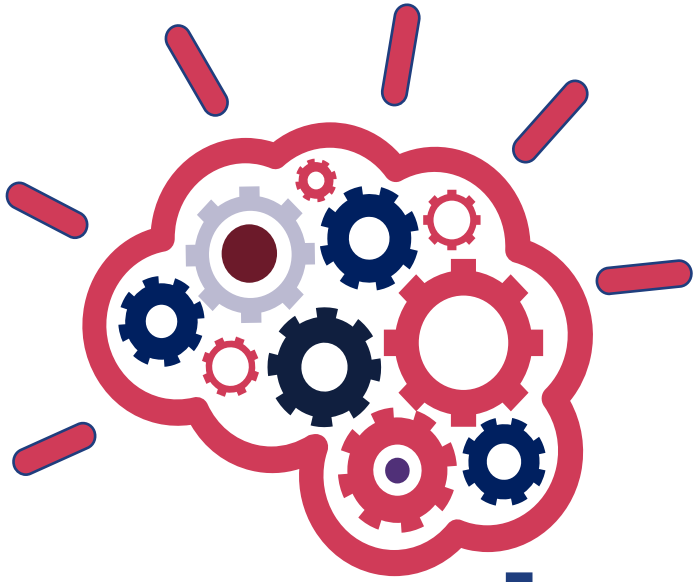
Reducing the CRA Regulatory Burden

Problem Statement

The Cyber Resilience Act is a piece of regulation with massive impact on the market and with the promise of strengthening the security posture of the EU.

In order to work, it needs to be **well implemented**, well received and understood by the market.

How can we **facilitate** its complex implementation?
How to **reduce time to market** and **costs** while **easing compliance**?



ECSO

Understanding Certification and Compliance

The value of certification

- Build trust via future European cybersecurity certification schemes across industries
  - Calibrate security controls according to the risk-based assessment
  - Horizontal schemes to support sector specific needs
- Whole lifecycle, management of vulnerabilities and risk, etc.
- Assessment of the security claims according to the desired assurance level
- Surveillance of certified products and certificate validity lifecycle

Some challenges of the industry

Vendors

Maintaining compliance is tough. Components in a product might not be not all certified using the same schemes or at the same assurance levels

Monitoring suppliers' activities to meet a product's multi-certification requirements is not easy

- **It is not always easy to identify the best cybersecurity certifications meeting the business needs**
- **Achieving, maintaining and renewing accreditation for different schemes is time consuming and resource inefficient**

CABs

While the scope of some schemes is too narrow and unusable in multiple domains, others are too generic, complicated and expensive to implement

Many schemes are not cheap and have overlapping requirements with other schemes

Principles of Certification Composition

Objectives

- **Enable** efficient **re-use** of **certificates** and **evaluation evidence**
- **Decrease** certification **cost** and improve overall process **speed**
- Benefit horizontal components **specialised in application** domains
- Strongly **contribute** on the **time to market** of **products**

Composition is a key concept to support a Supply Chain of Trust

Composition for CRA Compliance

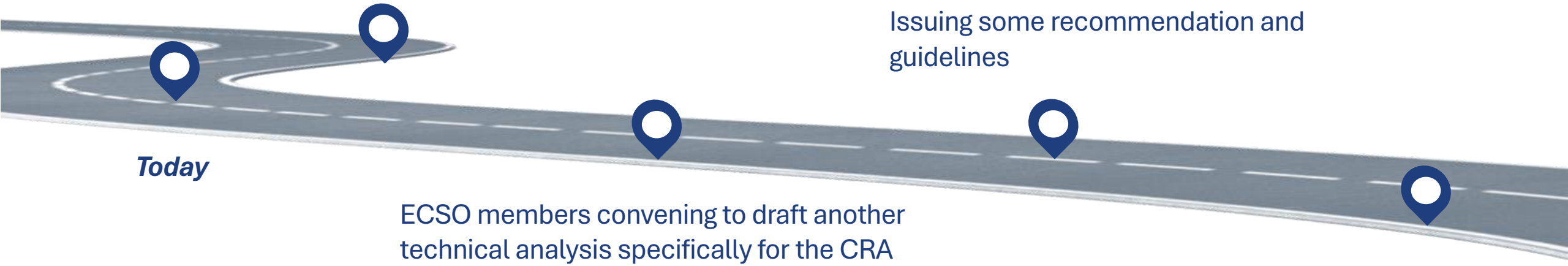
Tool to support the conformity procedure - Composition applies to regulations, standards, certifications; and it is effectively an example of simplifying the interplay between these elements.

CRA challenges for achieving composition - The composition for third party conformity assessment, for self-declaration, methodologies when dealing with composition, third part assessment, cybersecurity certification

Enablers for composition - What's missing for the national accreditation bodies, conformity assessment bodies (CAB), for the manufacturers (Open-source supply chain), for the market authority

Future Work Plan

Previous work
Technical analysis on “Product Certification Composition”



Today

ECSO members convening to draft another technical analysis specifically for the CRA

Issuing some recommendation and guidelines

Final Considerations

Ten Final Considerations

Preliminary suggestions for further investigation

1. Designate **one single point for reporting of ALL cybersecurity incidents**, beyond the NIS2 scope.
2. **Standardize 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 **Third Part Risk Management** (TPRM) **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. Develop more practical implementation guidelines on **CRA conformity assessments** (i.e., module B, C and H).
8. Draft horizontal guidelines for **CRA Composition.**
9. Develop methodological support documents for the **implementation of requirements**, focusing on a **bottom-up** approach lead by **technical experts** (e.g., asset criticality classification).
10. Continuously engage with a wide range of stakeholders including sectoral and cybersecurity associations, via awareness-raising sessions, public consultations, and webinars.

Open Discussion

Thank you!