ECSO
EUROPEAN CYBER SECURITY ORGANISATION

July 2025 v2

STREAMLINING REGULATORY OBLIGATIONS ACTION PLAN

ECSO STREAM
POLICY ANALYSIS
AND OUTREACH

ecs-org.eu

DISCLAIMER

COPYRIGHT NOTICE

ABOUT ECSO

The European Cyber Security Organisation (ECSO) is the non-profit membership-based organisation working for a more **resilient** and **strategically autonomous** Europe. Established in 2016, ECSO unites more than **320 stakeholders**, including companies of all sizes, research centres, public administrations, and many more. Organised in working groups supporting key industry areas, ECSO provides a platform for cooperation, informed decision-making, and **public-private collaboration**. *Click here to read more on the website.*

ABOUT THE ECSO POLICY ANALYSIS AND OUTREACH STREAM

The ECSO Policy Analysis and Outreach Stream delivers in-depth **policy analysis** to ECSO Members, helping them decode and act upon key European cybersecurity developments. The initiative involves close collaboration with EU policymakers and the integration of insights from both **public** and **private** sectors. By engaging with European and international stakeholders, it promotes **meaningful dialogue** for a structured, dynamic European cybersecurity landscape. *Click here to read more on the website*.

EMPOWERING EUROPEAN CYBERSECURITY COMMUNITIES

CONTENTS

INTRODUCTION

1.

1. Introduction to the action plan

Building on ECSO's long-standing engagement with EU cybersecurity policy, this document puts forward initiatives for European institutions to address, expanding on our preliminary suggestions for streamlining cybersecurity regulatory obligations. It includes key challenges, ranked in order of importance, and mapped against actionable recommendations clustered per type, and associated to responsible stakeholders, efforts foreseen, and priority suggested, based on professional judgment.

The actionable recommendations are divided in four groups:

- Incident reporting,
- Risk management framework,
- Supply Chain,
- Assessments and Auditing.

European Cyber Security Organisation (ECSO)

The European Cyber Security Organisation (ECSO) is the **pan-European**, private-public federation (**non-profit**) developing Europe's cybersecurity resilience and strategic autonomy. Established in 2016 as the European Commission's contractual partner for the **Public-Private Partnership in Cybersecurity**, ECSO unites more than 320 stakeholders, including businesses of all sizes, public administrations, and research centres, and provides a platform for dialogue, **knowledge sharing**, visibility opportunities, **industry advocacy**, and further public-private collaboration.

ECSO CISO Community

Additionally, ECSO manages a pan-European, cross-sector **CISO Community** comprising several hundred members who provide firsthand insights into the practical challenges of implementing current and forthcoming EU cybersecurity policy requirements.

ECSO research on streamlining regulatory obligations

For context, ECSO has been conducting research on regulatory burden and potential simplification since the summer of 2024. By bringing together national public administrations, operators, manufacturers, including service and solution providers who constitute and secure the core of the supply chain, testing laboratories, and CABs (conformity assessment bodies), leading assessments and audits, ECSO is uniquely positioned to offer the best possible insights into the challenges and good practices related to this topic.

Disclaimer

The information provided in this document is not intended to be considered as final or exhaustive.

We aim to regularly engage all parties, collect inputs, and present different views, which may at times result in further improvements or nuances.

The recommendations wording has been simplified to facilitate readability.

The stakeholders listed are not meant to be exhaustive either; many more stakeholders are expected to be involved, with varying degree of responsibility and engagement.

Next steps

As consultations led by the European institutions progress, ECSO is prepared to further dive into high-priority initiatives for regulatory simplification. ECSO stands ready to organise dedicated interviews and workshops, engaging additional stakeholders and developing a detailed breakdown of activities.

We invite ECSO members, CISO community members, and the broader cybersecurity ecosystem to reach out to us to share hands-on experiences or express strong dissenting views.

INCIDENT REPORTING

2.

2. Incident reporting

Context

Incident reporting requirements under evolving cybersecurity regulations pose significant operational and compliance challenges for entities. During an incident, organisations must balance incident response activities and the simultaneous preparation of regulatory reports, at times diverting resources from immediate response efforts to administrative compliance, according to some stakeholders. These reporting obligations often involve overlapping or unclear requirements across different authorities, resulting in duplicated efforts and inconsistent feedback received from authorities.[1] This complexity is exacerbated by tight timelines and limited internal capacity, particularly for medium-sized enterprises lacking dedicated compliance teams. Incident reporting calls for clarity, consistency, and proportionality.

Horizontal policies

NIS2, GDPR, eIDAS, CRA, CER.

Vertical policies

DORA, PSD2, Medical Device Regulation, European Electronic Communications Code (EECC), Network Code on Cybersecurity, any other relevant policy.

Key challenges

IR-1. Overlapping regulatory requirements mandating reporting information about the same incident under multiple regulatory frameworks, policies, authorities, and Members States.

IR-2. Uncertainty in determining when reporting obligations are triggered due to differing definitions of what constitutes a reportable incident.

IR-3. Significant complexity introduced by the need to notify the same incident to numerous authorities, sometimes exceeding 40 in highly regulated sectors[2].

IR-4. Operational strain caused by conflicting reporting timelines, such as NIS2's 24-hour deadline versus GDPR's 72-hour requirement.

[1] While inputs on incident reporting requirements have already been collected and presented in previous ECSO publications such as 'Streamlining Regulatory Obligations of EU Cybersecurity Policies', a more detailed mapping may be published in the future.

[2] The estimate reflects the financial sector's advanced maturity level and its comprehensive regulatory landscape. It illustrates a scenario involving a large, publicly-traded European financial institution experiencing an incident that spans all EU countries and affects its entire service portfolio, where the institution affected chooses to fulfil mandatory and voluntary reporting to maintain good offices and potential investigation support.

IR-5. Linguistic and terminological differences across member states, as key technical and legal concepts may have different meanings when implemented in national languages, leading to inconsistent compliance approaches and reporting practices.

IR-6. Additional reporting obligations imposed by supply chain relationships, expecting communication with partners and clients beyond regulatory authorities.

IR-7. Increased documentation burden resulting from inconsistent levels of detail required across regulations.

IR-8. Lack of standardisation in notification formats, ranging from emails to documents and online submission forms.

Actionable recommendations

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
1.	Governance and Strategic Coordination	Establish an EU Incident Reporting Task Force with representatives from all relevant authorities to develop a unified incident reporting framework.	IR-1, IR-3, IR-5	ENISA, EDPB, ESA, national CSIRTs, EC	High	High
2.	Regulatory Harmonisation	Develop cross-regulation mapping guides that help address and simplify overlaps between reporting requirements, enabling organizations to streamline compliance documentation and reduce redundant efforts.	IR-1, IR-3	ENISA	Medium	High
3.	Operational Standardisation	Harmonise incident classification guidelines with quantifiable metrics and examples.	IR – 2	EC, ENISA, national regulators	Medium	High
4.	Regulatory Harmonisation	Synchronise reporting timelines between frameworks establishing a common timeline progression from initial notification to follow-up reports.	IR-4	EC, ENISA, national regulators, ESA	High	Medium

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
5.	Operational standardisation	Standardise reporting templates and procedures that specify required fields, evidence formats, and technical taxonomies to ensure consistent information collection.	IR-8, IR-7	ENISA, national regulators, CSIRTs	Medium	High
6.	Operational Standardisation	Develop multilingual reporting capabilities and standardised terminology to overcome language barriers.	IR-5	EC, ENISA, national authorities, language services bodies	Low	Medium
7.	Cross-Border and Multi-Authority Coordination	Create a "report once, comply many" mechanism where a single report can satisfy requirements across multiple regulations and authorities.	IR-1, IR-3, IR-6	EC, ENISA, ESA, national authorities	High	High
8.	Operational Standardisation	Develop legally binding cross-recognition agreements between regulatory authorities to accept reports submitted under one regulatory framework as valid for others.	IR-1, IR-3, IR-4, IR-6	EC, Member States	High	High

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
9.	Technical infrastructure	Develop a central European reporting platform, where incidents are reported directly, while data is stored and managed by member states.	IR-3, IR-6 IR-8	EC, ENISA, national CSIRTs, data protection authorities	High	High
10.	Automation and Technical Integration	Establish secure API interfaces between organisational security tools and the European reporting platform to automate and expedite incident documentation.	IR-8, IR-7	ENISA, EC, cybersecurity vendors, national CSIRTs	Low	Medium
11.	Automation and Technical Integration	Establish clear feedback loops where authorities provide actionable guidance after reports.	IR-7, IR-2	National regulators, CSIRTs, ENISA	Low	Medium
12.	Technical Infrastructure	Fund the development of an open-source, EU-certified incident reporting tool that organisations can integrate with their security systems.	IR-8, IR-7	ECCC	Medium	Medium

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
13.	Capacity Building and Support	Provide regulatory sandboxes where organisations can test incident reporting procedures without penalties during implementation periods.	IR-2	EC, national regulators	Low	Low
14.	Capacity Building and Support	Create a dedicated SME support program offering technical assistance, specifically focused on reporting processes for smaller organisations.	IR-1, IR-7	EC, Member States	Medium	Medium

3. RISK MANAGEMENT FRAMEWORKS

3. Risk management frameworks

Context

As Member States transpose the NIS2 Directive into national legislation, entities in scope are required to implement security measures in compliance with risk management frameworks. However, the Directive itself does not prescribe specific frameworks or standards, leaving room for national discretion to align high level security measures to national specificities or existing frameworks. Notwithstanding the benefits of this approach, such as limiting disruption, enabling sector-specific tailoring, and granting member states full control over critical sectors, this has led to a fragmented regulatory environment, especially for cross-border organisations. These inconsistencies create operational inefficiencies, increase costs, and complicate internal risk management processes. Greater harmonisation and alignment of frameworks under NIS2 would support a more coherent and efficient cybersecurity posture across the EU, reducing the burden on entities while strengthening overall cybersecurity. The need for further harmonisation is also evident in the interdependence of infrastructures across sectors, for example, the energy and telecommunications sectors serve as enablers for numerous other critical sectors, underscoring the necessity of a coordinated approach.

Relevant policies

NIS2 Directive and DORA. Also applicable to any other European or national policy requiring a risk management process (e.g. Network code on cross-border electricity flows) with no harmonised standards.

Key challenges

RMF-1. Increased compliance costs driven by fragmented and evolving national legislation and framework requirements.

RMF-2. Lack of consistency across national risk management frameworks, with countries relying on either international standards or domestic approaches, making alignment difficult.

RMF-3. Duplication of effort for multinational entities, which navigate and comply with varying control requirements across jurisdictions, especially as wording or details may vary.

RMF-4. Significant time and resources required to map frameworks internally for compliance purposes, often without corresponding improvements in security outcomes.

RMF-5. Difficulty in monitoring and responding to frequent updates across multiple frameworks.

RMF-6. Limited value of high-level mappings, which may be missing out on specific details, since even minor technical differences (e.g. differences in encryption algorithm versions) can cause serious operational or business disruptions.

Actionable recommendations

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
1.	Regulatory Harmonisation	Publish cross-framework mappings ahead of compliance deadlines to support timely implementation.	RMF-3, RMF-5	ENISA	Low	High
2.	Cross-Border and Multi-Authority Coordination	Promote mutual recognition of security frameworks among Member States.	RMF-1, RMF-2, RMF-3	EC, ENISA Cooperation Group	Medium	High
3.	Automation and Technical Integration	Develop and promote tools for automated mapping of risk management frameworks.	RMF-3, RMF-4, RMF-5, RMF-6	ECCC, ENISA	Medium	Medium
4.	Regulatory Harmonisation	Rely on existing internationally recognised standards as a proof of compliance.	RMF-1, RMF-2, RMF-4	Member States	Low	High

SUPPLY CHAIN

4.

4. Supply chain

Context

Third-party cybersecurity risks are an undisputed source of concern for both regulators and organisations. As regulations evolve to cover supply chain providers, from DORA to NIS2, entities are increasingly required to demonstrate active management of the security implications of their supply chains. However, current practices for assessing supplier security risks are fragmented, resource-intensive, and often misaligned with the operational realities of small and medium-sized vendors. The absence of standardised approaches, together with a proliferation of inconsistent and overlapping security assessment practices like questionnaires, creates significant administrative burden without delivering proportional security improvements. Addressing these issues is essential to enable scalable, effective third-party risk management while supporting the competitiveness of EU-based suppliers.

Relevant policies

NIS2, DORA, CRA, Cybersecurity Act

Key challenges

SC-1. Lack of agreement on which frameworks to use, with existing ones often too burdensome for small and medium suppliers or further customised by individual companies.

SC-2. Absence of a standardised approach to assess supplier maturity.

SC-3. Limited visibility beyond tier-1 suppliers, hindering effective risk assessment and complicating enforcement across multi-tier supply chains.

SC-4. Disproportionate compliance burden placed on smaller EU vendors compared to larger international competitors.

SC-5. Difficulty in managing non-EU suppliers who may not understand or prioritise EU-specific requirements.

SC-6. Administrative overhead caused by lack of mutual recognition between risk management frameworks, combined with assurance expiration and renewal cycles.

SC-7. Complexity in verifying supplier compliance, particularly when suppliers lack clarity on requirements.

SC-8. Proliferation of overlapping, lengthy questionnaires with platform inconsistencies and varying formats.

SC-9. Resource strain and legal exposure resulting from time-intensive, legally binding questionnaires.

SC-10. Limited automation capabilities for continuous compliance monitoring.

SC-11. Absence of standardised, machine-readable formats for security requirements.

SC-12. Burdensome processes involved in updating supplier agreements to reflect evolving regulatory demands.

SC-13. Repeated requests for suppliers to complete security questionnaires during product or service procurement.

Actionable recommendations

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
1.	Governance and Strategic Coordination	Develop an EU Supply Chain Security Framework by consolidating effective elements from national schemes.	SC-1, SC6, SC-7	EC, Member States	High	High
2.	Capacity Building and Support	Integrate SBOM requirements into the EU Supply Chain Security Framework.	SC-3, SC-7, SC-10		Medium	High
3.	Operational Standardisation	Develop a methodology to classify and manage third-party suppliers.	SC-2, SC-5, SC-7	ENISA, Industry	Medium	High
4.	Regulatory Harmonisation	Specify baseline security controls and risk-based tiers.	SC-1, SC-4, SC-7	EC, ENISA, Industry	Medium	High
5.	Regulatory Harmonisation	Establish a consistent maturity scoring methodology across regulatory frameworks that is mapped to the risk level of services and products supplied.	SC-2, SC-6, SC-8	EC, ENISA, National Authorities	High	Medium

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
6.	Operational Standardisation	Enable mutual recognition and create equivalency mappings between EU national and major international frameworks.	SC-6, SC-5, SC-13	EC, Member States	High	High
7.	Operational Standardisation	Create a list of accepted certification schemes and labels as valid indicators of supplier security levels.	SC-6, SC-7, SC-13	EC, ENISA	Medium	Medium
8.	Operational Standardisation	Automate evidence mapping across multiple frameworks (e.g. NIS2, CRA, ISO, SOC 2), with the goal of pre-populating the majority of requirements.	SC-8, SC-9, SC-11	EC, Industry	High	Medium
9.	Technical Infrastructure	Develop and promote machine-readable formats for representing security requirements.	SC- 11, SC-8, SC-10	EC, Standardisation Bodies	Medium	Medium
10.	Automation and Technical Integration	Create a centralised EU supplier assessment database.	SC- 13, SC-8, SC-9	EC	High	High
11.	Cross-Border and Multi-Authority Coordination	Establish a standard contractual framework for supplier agreements.	SC-12, SC-5, SC-7	EC, Industry	Medium	Medium

ID	Type	Recommendations	Challenges	Stakeholders	Effort	Priority
12.	Automation and Technical Integration	Fund development of tools to enable visibility across multi-tier supplier networks.	SC-3, SC-10	EC, Member States	High	Medium
13.	Capacity Building and Support	Implement a “comply or explain” regime to ease compliance burdens for smaller entities.	SC-4, SC-9	EC, Member States	Low	High

ASSESSMENTS AND AUDITING

5.

5. Assessments and auditing

Context

In recent years, cybersecurity policies and laws enacted at both the EU and national levels have established stringent security requirements and related supervision schemes to ensure compliance. Although approaches vary across countries and policies, entities in the scope must establish or adjust their internal processes to manage compliance effectively. The expansion and increasing complexity of this ecosystem have resulted in significant efforts and resources needed to meet security compliance requirements. This presents challenges for both regulated entities and supervisors, lacking resources and trying to develop a risk-based, prioritisation approach.

Relevant policies

Any policies requiring assessments, auditing, or supervision, with a particular focus on NIS2 Directive, CRA, and DORA.

Key Challenges

AA-1. Excessive time and effort required for manual data collection during assessments and audits.

AA-2. High resource demands associated with conducting formal audits.

AA-3. Increased administrative burden and costs caused by outsourcing assessments or audits due to internal capacity constraints.

AA-4. Dependence on specialised expertise to conduct technical assessments and audits.

AA-5. Inefficiencies and inconsistencies resulting from text-based or spreadsheet-driven assessments.

AA-6. Limited accessibility to dedicated GRC tools due to high costs, excluding less-resourced entities.

AA-7. Variation in auditing approaches among different auditor professionals or auditing companies.

AA-8. Different supervisory approach between countries, varying from self-assessments to formal audits.

AA-9. Significant operational burden imposed by continuous monitoring throughout the product lifecycle.

Actionable recommendations

ID	Type	Recommendations	Challenges	Stakeholders	Efforts	Priority
1.	Governance and Strategic Coordination	Mandate the release of all mandatory security requirements in machine-readable format.	AA-1, AA-5, AA-8	EC, Member States	Medium	High
2.	Automation and Technical Integration	Develop security requirements in machine readable formats.	AA-5, AA-8	Member States, ENISA	High	High
3.	Operational Standardisation	Establish standardised formats for compliance reporting.	AA-5, AA-7, AA-8	EC, Member States	Medium	High
4.	Automation and Technical Integration	Develop tools to streamline assessments and manage compliance effectively.	AA-1, AA-3, AA-4, AA-5, AA-6, AA-9	Industry, Member States	High	High
5.	Capacity Building and Support	Invest in automation solutions to support compliance for relevant entities.	AA-1, AA-2, AA-3, AA-4, AA-5, AA-6, AA-8, AA-9	ECCC	Medium	Medium

ID	Type	Recommendations	Challenges	Stakeholders	Efforts	Priority
6.	Governance and Strategic Coordination	Run a feasibility study to identify success factors and challenges of automated compliance.	AA-4, AA-5, AA-9,	ENISA	Low	Medium
7.	Capacity Building and Support	Conduct pilot programs to test tools and processes, aiming for efficient and effective adoption.	AA-2, AA-6	ECCC	Low	Medium
8.	Regulatory Harmonisation	Accept proof of compliance via standardised formats.	AA-8	Member States	Medium	Medium
9.	Cross-Border and Multi-Authority Coordination	Recognise auditing authorities and reports across different countries.	AA-7, AA-8	Member States	Medium	Medium

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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