ENISA Advisory Group

On NIS2 Post Implementation

June 2025

AUTHORS

Annita Sciacovelli, Christine Skropke, Jos Helmich, Silke Holtmanns, Daniel Schatz, Alessandro Menna, Thomas Rosenzweig, Sebastiaan van ‘t Erve, Ilias Chantzos, Katja Kmet Vrčko

ACKNOWLEDGEMENTS

Main drafting lead by Annita Sciacovelli, Christine Skropke, Jos Helmich. ENISA activity manager support by Marnix Dekker

TABLE OF CONTENTS

1. INTRODUCTION

The ENISA Advisory Group (AG) decided in its meeting of 15 September 2023 to draft an AG opinion paper on “NIS2 Directive post-implementation”. In this opinion paper the AG takes a high-level perspective on the NIS2, post the NIS2 transposition deadline, and makes specific recommendations to ENISA and other stakeholders, about how to ensure that the NIS2 is implemented successfully, and how to best reach the goals of the NIS2, and to reach a high-level of cybersecurity across the EU. Note that opinions issued by the AG are in no way binding for ENISA and do not represent the official opinion of ENISA, nor does ENISA bear any responsibility for opinions issued by the AG.

1.1 SCOPE AND GOAL

The scope of this opinion paper is the NIS2 transposition and implementation by the EU Member States, post transposition deadline, including aspects like:

- Good practices and lessons learnt around compliance with the NIS2 provisions by the entities in scope of the NIS2, and especially smaller entities
- The impact of NIS2 provisions on the resilience of NIS sectors, and their level of cybersecurity investments
- Good practices and lessons learnt from regulatory compliance between NIS2 and other policy instruments, such as DORA

The goal of this opinion paper is to give strategic guidance to ENISA's Executive Director for the future of NIS2. This opinion paper does not intend to duplicate activities and outputs of ENISA’s work programme.

1.2 WORKING METHOD

ENISA, as secretariat of the AG, created a working group of volunteers from the AG, to work on the opinion paper:

- Annita Larissa Sciacovelli (rapporteur)
- Christine Skropke (rapporteur)
- Jos Helmich (rapporteur)
- Silke Holtmanns
- Daniel Schatz
- Alessandro Menna
- Thomas Rosenzweig
- Sebastiaan van ‘t Erve
- Ilias Chantzos
- Katja Kmet Vrčko

The rapporteurs acted as liaison with ENISA and moderated the working meetings.

1.3 BACKGROUND

We provide relevant background on the NIS2, and some recent ENISA reports relevant for this opinion paper:

- **NIS2:** The NIS2 was adopted in 2022, the transposition deadline was 17 October 2024.

- **NIS2 implementing rules:** The Commission specified detailed incident reporting and security measures in cross-EU NIS2 implementing rules - The Commission also asked ENISA to publish a technical guideline for the NIS2 security measures, which was consulted with industry and is now published at (to do – due to be published shortly).

- **NIS2 transposition status:** At the time of writing a few (~8) countries have transposed the NIS2. A large number (~19) of Member States are in advanced stages of transposition and are expected to have transposed before the end of 2025[1].
  - For example, Belgium was one of the first countries to transpose the NIS2 and it created a Cyber Fundamentals (CyFun) Framework to support entities in scope of NIS2 with guidance on how to do risk assessment and how to take appropriate security measures.
  - For example, Italy transposed the NIS2 via a decree in 2024 and the registration deadline for entities in scope of the NIS2 was 1 December.

- **ENISA NIS strategy:** ENISA as part of its 3-year (2023-2025) NIS strategy, allocated budget and resources to support and enable a rapid implementation of the NIS2, balancing between horizontal and sectorial **activities**. Under the ENISA NIS strategy, ENISA implemented its new tasks under the NIS2, for example the EU registry for digital infrastructure (EUDIR), the EU vulnerability database (EUVD), supported MS with their NIS2 tasks, for example by providing technical guidelines for NIS2 incident reporting and NIS2 security measures.

- **EU State of the Union report:** The EU state of the Union report, a new ENISA task under the NIS2, was published at the end of 2024. It recommends
  - Harmonized, timely and coherent implementation of EU cybersecurity policies
  - Blueprint revision to improve the EU response to large-scale incidents, and the cybersecurity capabilities at national and EU level
  - Strengthening the EU cyber workforce, by implementing the Cybersecurity skills academy
  - Addressing the cybersecurity of the EU's ICT supply chain with a horizontal policy framework for supply chain security
  - Addressing sectorial issues, to improve the maturity of NIS sectors, and to use the Cyber Solidarity Act to improve sectorial preparedness and resilience.
  - Promoting a unified approach to raising cybersecurity awareness and cyber hygiene among professionals and citizens.

- **ENISA NIS investments:** The yearly ENISA NIS investments report surveys ~1350 companies across the EU about their cybersecurity maturity, their challenges, and their cybersecurity investments. The main conclusions of the 2024 NIS investments report
  - Companies earmark, on average, 9,0% of IT investments for cybersecurity, a 1.9% increase compared to last year.
  - Companies allocate, on average, 11.1% of IT FTEs for cybersecurity, a 0.8% decrease
  - 80-90% of companies expect to need more cybersecurity staff to implement the NIS2, CRA, DORA and the network code cross-border electricity flows.
  - In 51% of companies, leadership participates in dedicated cybersecurity trainings.
  - 90% of entities expect an increase in cyberattacks in the coming year.

[1] https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive

Beyond the NIS2, there are other EU initiatives important to mention:

- **CER** – The Critical Entities Resilience Directive, was adopted in parallel with the NIS2 – is the general overarching EU directive for the resilience of critical sectors, both for the purely physical threats and for the ICT infrastructure. The NIS2 is *lex specialis* under CER and deals with all-hazard threats for the ICT in the critical sectors. Member States are implementing NIS2 and CER almost in parallel. Under CER MS have to identify critical entities by July 2026.
- **CRA** – The Cyber Resilience Act, adopted in 2024 – introduces a cyber labelling framework for products with digital elements. The CRA supplements the EU certification framework for some specific high-risk categories of products.
- **CSOA** – The Cyber Solidarity Act adopted in 2024, introduces cyber reserve funding mechanism (a continuation of the ENISA support), an incident review mechanism, and a network of cyber hubs for public to private threat intelligence sharing.
- **DORA** – The Digital Operational Resilience Act, the EU regulation for resilience of the EU's finance sector, came into force in 2024 and the EBA issued the DORA Regulatory Technical Standards (RTS), which contain technical cybersecurity requirements for the sector. EBA is also using the ENISA incident reporting tool CIRAS developed for the NIS incident reporting.
- **Sectorial cybersecurity requirements** – There are various sectorial rules under the NIS2, and other sectorial initiatives with relevant cybersecurity requirements, such as the Network code for cross-border electricity flows, the Radio Equipment Directive (RED), the EU 5G toolbox, the Medical Devices Regulation (MDR), and Directive 2012/18/EU on the control of major-accident hazards involving dangerous substances.

2. OBSERVATIONS AND RECOMMENDATIONS

2.1 NIS2 COMPLIANCE CHALLENGES – THE NEED TO HARMONIZE BETWEEN MS

In 2015 the European Commission conducted a review of the NIS1, using the Better Regulation Guidelines. The increasing interdependencies and dependencies with non-covered sectors and the wide margin of discretion in defining the scope of the NIS1 in the Member States were emphasised as a problem. The report about the review noted that some NIS provisions were not clearly defined and allowed member states too much room for manoeuvre in national implementation. The review concluded that the NIS1 was in danger of failing to fulfil its objective of ensuring a well-functioning EU internal market. The NIS2 was proposed to reduce inconsistencies in the internal market by harmonising the scope of application, security and incident reporting requirements, national supervision and enforcement, and the capacities of competent authorities".

Although only a few member states have transposed the NIS2 into national law at the moment, it seems there will still be some divergence in the NIS2 transposition, in terms of sectors in scope, and horizontal or sectorial security requirements, which poses challenges for entities operating in the EU internal market. For instance, the Czech Republic also includes the military industry, while Poland has expanded the energy sector to include sub-sectors such as mineral extraction. Hungary introduced risk classes, with different requirements for each class of entities, deviating from the NIS2 approach of categorizing entities as "essential" and "important." Germany, meanwhile, retains an additional "KRITIS" layer for particularly critical services, which must adhere to stricter requirements. Austria requires a more comprehensive list of risk management measures than in NIS2 Article 21, and most other member states. Belgium developed its Cyber Fundamentals Framework (CyFun) as a compliance guide, which, aligns with major frameworks like ISO27001 and NIST CSF, but is not identical to these frameworks and adds yet another layer of complexity for cross-border entities.

Recommendation 1 - Develop one cybersecurity baseline for the NIS2: ENISA should develop a single cybersecurity baseline for the EU and promote its use by the EU Member States. The technical guideline for NIS2 security measures for the digital infrastructure sector, can be used as a basis. One approach could be to have one foundational/horizontal baseline and then create limited sector-specific additions.

Consider for example an EU company, providing services and selling products across Europe. NIS2 compliance in its home country A is often not considered sufficient by a potential buyer in country B. The SME would need to demonstrate to customers also to be NIS2 compliant.

Recommendation 2 - Enable re-use of national approaches to NIS2: ENISA should collect the different requirements in the different MS approaches to the NIS2, and promote mutual recognition, for example by mapping requirements. For example, several countries have said they appreciate the Belgian Cyber Fundamentals (CyFun) framework and are considering to reference/recognize it.

Important to note, that a mutual recognition principle exists in EU law. It applies in the field of free movement of goods. Where no harmonised rules exist at European level, products lawfully marketed in one Member State can be sold in other Member States regardless, of complying or not with the national technical rules of these Member States. Member States mutually recognise that national technical rules are equally protecting the public interests pursued. This principle was first applied in the landmark Cassis de Dijon ruling (Case C-120/78) by the European Court of Justice.

2.2 NIS2 COMPLIANCE CHALLENGES – THE NEED TO ALIGN BETWEEN SECTORS

The implementation of NIS2 is also facing some challenges by the overlapping of scope between sector-specific regulations and existing business models. The NIS2 is intended to be an all-encompassing legislation that is addressing the security of critical infrastructure and lays out the security best practices that industry should apply. The adoption of sector-specific requirements, while necessary in certain circumstances, should happen in a manner that clearly delineates the additional obligations and does not create duplication or conflicting requirements.

For instance, the simultaneous application of DORA, NIS2 and GDPR results in three different breach notification regimes. Moreover, there are scenarios in which a third-party ICT service provider falls under DORA, but also under NIS2 as cloud provider or MSP subject to the NIS2. Car manufacturers, for example, are subject to NIS2 as manufacturers, but also in scope of DORA, for their insurance and leasing services they provide when selling their vehicles.

This means many companies are dealing with a multitude of cybersecurity requirements, stemming from multiple horizontal and sectorial policies, supervised by a multitude of authorities. Even without considering cross-border operations, and the differences between the 27 different EU countries, explained in the previous point.

Recommendation 3 - Map between the NIS2 horizontal baseline and sectorial rules: ENISA should identify and map between the NIS2 and the different sectorial security measures and incident reporting requirements, such as those under DORA.

Recommendation 4 - Map between NIS2 and widely known international standards: ENISA should map the NIS2 requirements to existing international standards, such as ISO27001, and NIST CSF. The mapping should work in both directions.

Recommendation 5 - Cross-sector regulatory coordination: ENISA should facilitate exchange of good practices between different sectorial authorities, and facilitate coordination of their different regulatory approaches. ENISA should ensure that sectorial policy implementation is fully aligned with the horizontal NIS2 framework.

Recommendation 6 - Common control taxonomy, technical repository: ENISA should create a common taxonomy of security controls, used in the different policies and frameworks, and identify gaps and overlaps.

2.3 NIS2 COMPLIANCE CHALLENGES – THE NEED TO SUPPORT SMALLER COMPANIES

Many smaller companies who are perhaps not themselves directly in scope of the NIS2, still have to deal with NIS2 compliance issues, for example because they are in the supply chain, providing services or products to entities in the NIS2 scope. Some countries have adopted simplified frameworks for smaller entities.

Recommendation 7 - Develop a NIS2-light framework for smaller companies: ENISA should also develop a NIS2-light framework for smaller companies, such as SMEs. ENISA should collect different SME frameworks in use in the MS, and develop a single reference framework/mapping.

To support especially smaller companies, it is also important to support the broader ecosystem of experts, solution providers and service providers, both at national and EU level.

Recommendation 8 - Support the NIS ecosystem and promote funding opportunities: ENISA and Member States should not only set the rules, but also support the broader NIS2 ecosystem. ENISA should promote existing EU funding programs, which can be used to support the implementation of the NIS2 requirements.

Because not all companies have the same resources or capabilities to implement NIS2 requirements, especially those offering services in newly introduced sectors, it would be advisable to support them with financial incentives, and eventually with tax incentives. This approach would promote fairness and help prevent security gaps.

Recommendation 9 - Consider cybersecurity financial incentives and tax breaks: ENISA should support MS with exploring and establishing financial incentives for improving cybersecurity, and consider for example tax breaks for investments in cybersecurity and resilience.

2.4 NIS2 AND SUPPLY CHAIN SECURITY – SUPPORTING ICT SUPPLIERS, SECURING ICT SUPPLY CHAINS

The Draghi report recognises the need to establish a strong and competitive market on cybersecurity in Europe that will enable the vision of open, strategic autonomy for the EU and its Member States. At the moment the EU's supply chain is heavily dependent on third countries, such as China. Considering the rapid geopolitical changes, this puts Europe's critical sectors at risk. It is crucial for EU policymakers to find ways to support the EU's own supply chain, and support the EU's ICT vendors.

A major obstacle for ICT vendors in the EU is the bureaucracy and overhead and the compliance burden in the different countries and in the different sectors. In the future, when the recently adopted CRA comes into force, ICT vendors in the EU will have to comply with CRA requirements, but also with NIS2 requirements, if they fall in a NIS sector and if they sell to customers in a NIS sector.

Recommendation 10 - Align and harmonize between CRA and NIS2: To ensure that EU vendors under the NIS2 and under the CRA do not have a double compliance burden, there is an urgent need to harmonize and align between the NIS2 and the CRA – for example when it comes to security measures, and to align the vulnerability and incident reporting processes as much as possible. For example, an

important consideration for the implementation of CRA implementation is the CRA application to cloud, and the overlap between cloud under CRA and cloud under NIS2.

A second obstacle for EU vendors is the plethora of different cybersecurity requirements coming from their customers, being national governments, or companies in the private sector, if all their customers use different security requirements in their procurement. A common approach to procurement, a cross-EU framework, like FEDRAMP, should be developed, to harmonize the procurement process and clarify the division of responsibilities between vendors and customers. Even in the US procurement is considered an issue, as discussed in the NIST Workshop on Enhancing Security of Devices and Components Across the Supply Chain (February 2025), the cybersecurity maturity of different suppliers varies widely. A single EU procurement framework could avoid a lot of unnecessary overhead on the side of the ICT vendors, and even simplify procurement on the buyer side. If different member states and different companies use different requirements in contracts, this would fragment the single market.

Recommendation 11 – EU Cybersecurity Supply Chain Framework (SupplySec): ENISA should develop a European Supply Chain Security and Procurement Cybersecurity Framework (SecProc), including a baseline of cybersecurity measures and a unified "due-diligence" methodology, which supports customers in securing their supply chain, reduces administrative burdens for suppliers, especially for those serving multiple customers across the EU, and simplifies the procurement process for EU customers, when they buy European.

This framework would not only help the ICT vendors but could also help the entities under the NIS2 in addressing ICT supply chain risks. ICT supply chain risks are a new focus in the NIS2, and were also identified as one of the rising trends in the latest ENISA Threat Landscape report. The supply chain of critical infrastructure providers includes materials, hardware and software. From a cyber security perspective software supply chains are difficult to manage, as there might be many contributors (potentially from high-risk countries), open source, proprietary code which is not disclosed etc. The supply chain consists of smaller and larger players. NIS2 wants to improve the resilience against supply chain attacks. This means there is a need to strengthening it is own ICT suppliers, deal with the risks of ICT supply chain in untrusted third countries, and make full use of its trusted ICT supply chain partners. Meaning trusted third countries with similar values, a similar approach to cybersecurity and resilience, such as the US, the UK, Japan, Taiwan, and South Korea.

Recommendation 12 – Partner with third countries with important ICT supply chains: Under its current international strategy, ENISA focuses mainly on the US and EU candidate countries. Considering the geopolitical changes, for example the ongoing trade and tariff wars, ENISA should also develop partnership with other countries, such as UK, Japan, Taiwan and South-Korea, which have an important ICT supply chain, and Canada, and Australia, who face similar issues as the EU.

The procurement framework should also facilitate a simple risk assessment of suppliers carried out by customers. Additionally, the framework could address (and standardize) the approach to contractual liability, capping damages, and others. It is important to reuse the widely used cybersecurity maturity framework CMMC[2].

Recommendation 13 – Develop NIS2 ICT Procurement baseline: As part of the SupplySec framework**,** ENISA should develop a NIS2 procurement baseline, with guidance and a baseline of minimum requirements for contracts with suppliers, standard clauses, give practical examples, for instance widely used labels, common security testing approaches, and include a simple risk assessment method so customer can evaluate suppliers and vendors.

[2] https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

One possible approach is to develop concrete security performance indicators into the standard contract clauses, related to vulnerability, and incident management, software development practices, security maturity assessment, existence of hardening guide/architecture, security support for the whole lifecycle, security testing coverage, security acceptance. Example cybersecurity contract clauses could help harmonize business practices and be helpful especially for SMEs. Widely used international reference standards should be mapped with product types, for example ISA 62443-4-1 for OT (Operational Technology), OWASP for web software, etc. This would avoid wide deviations and "spontaneous contractual creativity" and immense burden for both the ICT vendors and the customers.

There may be a need for guidance and alignment on monitoring and testing in the context of procurement: Security testing of software should be documented and it should be relatively for customers to replicate and monitor the security behaviour of products in the testing or production environment to discover low quality security. Findings in the monitoring can be reported back to procurement. Monitoring and testing guidance would support IT and operational departments, enable an audit trail and make it easier for the buying party in the supply chain to identify issues and potentially monitor intensively high-risk suppliers.

An important aspect here is cybersecurity requirements for the procurement of OT – Operational Technology, which is quite different from IT, and often used in critical sectors. NIS2 includes implicitly OT as part of the ICT supply chain. In the moment there is a lack of understanding, what OT suppliers should certify or comply against in their role as suppliers, ISA/IEC 62443 is quite large and often does not fit for SMEs. This leads to the evolution of very diverse understanding and market fragmentation. Clarification and at least high-level guidance on OT security requirement as part of NIS2 would be good.

Recommendation 14: Develop NIS2 OT procurement guideline: As part of the NIS2 ICT procurement guideline, ENISA should develop specific recommendations for secure procurement of OT.

2.5 NIS2 INCIDENT REPORTING – MAKE REPORTING MUCH EASIER

Historically, mandatory incident reporting was first introduced in safety regulations, in areas such as nuclear safety, offshore safety, and aviation safety. Reporting helped to understand root causes of incidents, to avoid repetition of failures, driving continuous improvement. Cybersecurity incident reporting to national authorities is an important part of the NIS2, enabling ex-post and ex-ante supervision by the national authorities, to ensure that entities take appropriate security measures (which is the core duty of the authority/regulator), and to drive continuous improvement in the sectors. Incident reporting also plays an important part role in business-to-business contract negotiations between an ICT supplier and customers, who need reports about issues with services or components they rely on. The fact that a company has reporting obligations, may even complicate contract negotiations.

Overall incident reporting can be a tricky and time-consuming process for a company, depending on the setting and the complexity of the incident. Generally speaking, incident reporting entails significant costs and human resources for a company, and it requires a solid process to understand all the legal implications and the business risks. Incident reporting often requires a broad investigation, involving experts across the organisation, for instance to do root cause analysis and impact assessments. Although there are many technical aspects to the process, the reporting process itself is often a rather legal task, handled by a legal/compliance team. It can also be challenging to meet tight incident reporting deadlines, such as the tight 24 hours initial notification obligation, especially when incidents are more complex. Inevitably, with a tight deadline, companies will focus more on the deadline for the report than the accuracy and the content of the report. In fact, it is now a good practice in ICT contracts to require a supplier or service providers to notify incidents which the customer would likely have to

report to authorities. And this should be considered also in the above-mentioned supply chain framework and procurement guidelines.

Often a single incident report is not enough. Most companies, especially service providers and ICT suppliers have to report incidents to multiple different authorities, different deadlines, using different thresholds and different reporting templates. For instance, NIS2, DORA, MDR, GDPR, and soon also CER, and CRA, will require some form of incident reporting to authorities. These different reporting processes are often not aligned, for example having different timings. The NIS2 has a 24 hours deadline for the first notification, the GDPR has a 72 hours notification deadline for data controllers, DORA RTS has a notification obligation deadline of 4 hours, if the incident is “major”.

Recommendation 15 – One reporting point, one template, one process: ENISA and MS to promote and pursue simplification of cyber incident reporting, both at national and EU level. ENISA should promote alignment and integration of the different reporting processes, and promote a single template or standard modules, for the cybersecurity aspects of incident reports.

For example, In Finland supervision over the different NIS sectors is decentralised, however one organisation, Traficom, acts as a single contact and coordination point. The national CSIRT, a part of Traficom, will play a key role in monitoring and analysing cyber threats, becoming the place to go to when problems occur.

Recommendation 16 – Increase the value of NIS2 reporting: ENISA should increase the value of NIS2 reporting both for national authorities and for the companies, by collecting reported incidents, and giving data and analysis back to the different horizontal and sectorial stakeholders.

2.6 STANDARDS AND CERTIFICATION FOR NIS2 - NIS2 AS AN EU LABEL

Article 25 of the NIS2 promotes the use of European and international standards to implement the cyber risk management measures of NIS2 Article 21. The importance of using European and international good practices is illustrated by the following example. In Germany for example, the national agency uses the IT Grundschutz framework for basic security, which has to be used in bids for government tenders. But, of course, Finland does not use IT Grundschutz, so for a Finnish company it would be difficult to go for bids in Germany. EU wide standards and frameworks would enable more competition and cross-border activities.

The NIS2 security measures should cover both IT, the OT, and cloud environments. For IT and OT, different standards are needed. For the IT part, to get a good baseline level of cybersecurity, companies often implement the ISO/IEC-27001 standard. However, for OT for example in factories, the ISA/IEC-62443 standard is often used, which prioritises availability more. ISA/IEC-62443 covers most NIS2 requirements and is particularly suitable for global companies. The NIS2 caused a shift in thinking at ISA, integrating more with ISO/IEC-27001, to benefit from the good practices used in IT. The relation between IT security and cloud security is also complex, because many companies are both cloud consumers, and cloud providers. The NIS2 security measures need to incorporate both aspects.

Business-to-business contracts between large companies often require an audit of all controls through independent auditor’s assurance report, following ISAE3402. This often becomes a de facto “license to operate”. On top of this, companies often need to demonstrate compliance with

other established frameworks such as ISO 2700x, SOC2, and PCI-DSS. Due to the costs of the associated audits of controls, this may, over time, create a glass ceiling between, on one hand the large businesses, and on the other side, the SMEs for which the compliance costs are often prohibitive. Without audits, however, there is a risk that certification becomes a glossy consumer-aimed sticker with no real security behind it. A light-weight assurance process is needed to help smaller business create and market their IT products in the internal market, on their own. Without it, the EU's innovation landscape would be impacted, favoring only the much larger companies.

As mentioned already, many SMEs that are caught in the slip stream of NIS2 entities, risk being faced with steep compliance costs, for instance they may be pushed to get an ISO-27001 certification. A more light-weight and less costly certification would be a solution especially or smaller companies. The Belgian CyFun scheme is one way to avoid unnecessary costs and provides the ability to increase the overall security posture of certified companies, and the overall supply chain. This would still allow regulators to supervise ex-ante or ex-post, specific resilience issues, specific controls, without having to audit all controls.

Recommendation 17: EU NIS2 label: ENISA should build on the NIS2 and explore the development of a NIS2 cybersecurity labels for organisations, to allow companies to re-use their NIS2 compliance, in also in their business-to-business interactions, nationally and cross-border.

3. CONCLUSIONS

We are now a few months after the NIS2 transposition deadline, and most EU Member States are still implementing and transposing, and a lot will depend on the details of the NIS2 implementation by the Member States, but some things already stand out. In the paper we made a number of specific recommendations, and we conclude with some more general considerations around the NIS2:

Use the NIS2 to make cybersecurity much simpler and an advantage for EU companies

Although less than under the NIS1, when it comes to NIS2 security measures and NIS2 incident reporting there is still unnecessary divergence and misalignment, from country to country and from sector to sector. In this opinion paper we made a number of specific recommendations to streamline, simplify, harmonize and align. Now is the chance for the EU Member States to build on the NIS2 and use this as a launch pad for developing *One cybersecurity framework for Europe, beyond NIS2,* and avoid a situation where companies have to work with a multitude of different frameworks and approaches, for each country and for each legislation, or policy area. Making NIS2 compliance into an EU label that businesses can use also vis-a-vis other businesses, would turn the NIS2 compliance overhead into an opportunity for businesses and economic growth.

Use the NIS2 to promote a phased building up of cyber resilience

Often when discussing the NIS2, the word compliance is mentioned, suggesting that companies now need to invest, to reach a start level of cybersecurity and resilience, by a certain deadline, to be compliant. With such a compliance focus, there is a risk that companies create a cybersecurity program where documentation is abundant, processes and policies are poorly understood, inconsistently applied, leading to siloed and audit-driven security, incident handling that is reactive, and policies that are being followed “on paper" but not in practice. What is much more important however, especially because technology and threats change rapidly, is that the EU Member States use the NIS2 as a framework for triggering, monitoring and overseeing continuous improvement by companies in the critical sectors. A step-by-step approach, for example, by addressing a few risk scenarios at a time, should be used at national and EU level.

Use legislative modularity, lego blocks, across different cybersecurity policies

The last years we have seen several major cybersecurity policy files were proposed and they are now being implemented. Too often however *each policy area is operating in silos* and taking different approaches – the left arm doesn’t know what the right arm is doing, or insists on doing things differently. For example, the rules for cloud, 5G networks, fixed telecom networks, are all different, already at the EU level, but also at national level the authorities and rules are often different. There is a future risk that also the CRA deviates from the NIS2, creating different groups, developing a large number of new standards, involving different national authorities for the supervision, etc. The EU should take a much more modular approach, re-use the relevant parts from one legislation, to avoid creating a jungle of different and overlapping rules and making Europe a very complex and costly place to do business.

Outlook towards NIS 3.0

Finally, a brief reflection on a potential future NIS3. Maybe there shouldn’t be a NIS3, but new cybersecurity initiatives are definitely needed. First of all, instead of creating even more rules, a

cybersecurity portfolio clean-up action is needed. For example, under DORA, the EU introduced a large number of very detailed cybersecurity requirements (DORA RTS). There are now many other sectorial policies, each drafting different security requirements for different sectors. The same happens on the side of products: There is now RED (Radio Equipment Directive), the Machinery Regulation, the Medical Device Regulation (MDR), and the CRA will come into force soon. The EU must bring order and alignment into all these EU Acts and directives affecting cybersecurity. Of course, we also believe there may be benefits to further harmonisation of the NIS2 implementation by the MS and that when the NIS2 is reviewed, and discussions about a potential NIS3 start, instead of a directive, perhaps an EU regulation should be considered, to simplify the work for both MS and companies.