CYBERSEC
EXPO & FORUM

ELIMINATING DIFFICULTIES AND CHALLENGES IN IMPLEMENTING LEGISLATIVE SOLUTIONS IN THE AREA OF CYBERSECURITY – DORA, NIS2

POLICY BRIEF

Table of contents

Dear Ladies and Gentlemen,

This document is the second *policy brief* resulting from the letter of intent signed during **CYBERSEC EXPO & FORUM 2024** on June 19th in Kraków, in the presence of Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski. The agreement was concluded between the **Kosciuszko Institute** and the **European Cyber Security Organisation (ECSO)** regarding the organization of a series of events focused on the priorities of digital and technological policy during Poland's Presidency of the EU Council.

The second meeting in the *Road to the Polish Presidency* series was dedicated to addressing challenges and overcoming obstacles in implementing legislative solutions in the field of cybersecurity, specifically **DORA and NIS2**.

In recent years, the European Union has significantly expanded its regulatory framework in the fields of cybersecurity and digitalization, reflecting its goals of building a more resilient and secure digital space. These efforts stem from the increasing reliance on digital infrastructure, the growing threat of cyberattacks, and an evolving cyber threat landscape that encompasses both criminal activities and state-sponsored actions. Additionally, geopolitical tensions, such as the war in Ukraine, have underscored the importance of robust mechanisms to protect critical infrastructure as well as the data of citizens and businesses.

Following years of debate and consultation, a series of comprehensive cybersecurity regulations have been introduced, including the NIS2 Directive, the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act (CRA). Each of these measures was designed to address specific gaps in the system. However, the implementation process has revealed challenges that confront the theoretical assumptions of the regulations with the practical realities of their application.

Drawing from the meeting held on November 21, 2024, attended by representatives of the Ministry of Digital Affairs Poland, Permanent Representations to the EU, the private sector, SMEs, ECSO, and the Kosciuszko Institute, as well as the research prepared by ECSO and KI, together we were able to identify key challenges regarding the implementation, harmonization, incident reporting and policy and strategy.

We would like to extend our deepest appreciation to all members of the working group whose unwavering commitment, expertise, and insights have been instrumental in the creation of this document. The resulting recommendations mark an important milestone in fostering a secure and digitally resilient society.

Our sincere gratitude also goes to the Ministry of Digital Affairs for their exceptional support and dedication, which has been vital to the success of this initiative, and a special thanks to Wojciech Berezowski. We are truly grateful for their professionalism, collaborative approach, and invaluable contributions, all of which have been key in advancing our shared mission.

We would also like to express our gratitude to the European Cyber Security Organisation (ECSO) for their months of dedicated effort and unwavering commitment. Our collaboration, expertise, and continuous engagement have been invaluable throughout this process. By providing meaningful input, facilitating collaboration, and sharing their extensive knowledge, ECSO has played a key role in shaping the outcomes of this initiative.

We would also like to extend our appreciation and thanks to our partners: Deloitte and Amazon.

Deloitte.

Members of the working group:

1. **Wojciech Berezowski** – Cybersecurity Counsellor in the Ministry of Digital Affairs of Poland
2. **Sebastijan Čutura** – European Cyber Security Organisation
3. **Marietta Gieroń** – The Kosciuszko Institute
4. **Paulina Górska** – The Kosciuszko Institute
5. **Łukasz Jędrzejczak** – Deloitte
6. **Eliza Kotowska** – The Kosciuszko Institute
7. **Eva Martinicova** – Amazon
8. **Matteo Molé** – European Cyber Security Organisation
9. **Szymon Mozel** – Deloitte
10. **Joanna Świątkowska** – European Cyber Security Organisation
11. **Cristian Michael Tracci** – European Cyber Security Organisation
12. **Maria Tsani** – Amazon

Please note that the challenges and recommendations outlined in this document are the outcome of collaborative discussions and do not represent the official positions, endorsements, or commitments of individuals and organisations contributing to the working group. They are intended solely for informational and exploratory purposes.

CHALLENGES

THE MOST CHALLENGING AREAS TO COMPLY WITH

Based on the survey conducted by the European Cyber Security Organisation (ECSO), the areas presenting the greatest compliance challenges 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**
- **heavy compliance procedures, including audits and certifications**

COMPLEXITY OF REGULATIONS

The complexity of the EU regulations has steadily increased in recent years, particularly with the introduction of frameworks like the Network and Information Security Directive (NIS2) Directive and the Digital Operational Resilience Act (DORA). Both policies serve as evidence of the efforts to strengthen digital resilience and enhance cybersecurity across the Member States.

However, the boundaries between NIS2 and DORA are not always well-defined, often creating uncertainty about which regulation applies to specific companies and what measures they must implement. This lack of clarity frequently results in gaps or inconsistencies in applying the required security standards. Entities encounter significant operational challenges when striving to comply with both existing and emerging regulations. These challenges span nearly every domain of cybersecurity, with variations influenced by factors such as the entity's maturity level, geographical location, and market positioning.

The NIS2 directive-based framework requires organizations to manage diverse national interpretations and implement schedules across member states. Companies must contend with differing definitions of scope, security standards, reporting requirements and supply chain regulations, which adds significant complexity to managing security and monitoring compliance in cross-border operations.

LACK OF HARMONIZATION

The fragmented regulatory landscape with variations across national and European required frameworks and standards, such as ISO and NIST, presents a significant challenge to achieving harmonization in cybersecurity compliance.

While the overarching goals of these regulations often align, detailed application does not always do so. In some cases, the new regulatory obligations contradict each other. This creates legal uncertainty for all stakeholders: business, public administration, civil society, and end-users. Each actor in the chain is forced to reconcile how to implement and apply overlapping or opposing regulatory rules. Issues such as reporting timelines, identifying the correct responsible authorities, duplication of information sharing, and continued confidentiality and security of any shared information pervade the multiple reporting regimes established under EU law.

One of the main challenges is the lack of a true harmonized regulatory approach across the Union. The current framework not only comprises different rules, but it does so as a minimum harmonization measure. This allows Member States to supplement requirements or impose national jurisdiction over products and services, compromising the simplifications that policymakers introduced in the new Directives. This is most evident in the case of the new Network and Information Security Directive from 2022 (NIS2).

The general objective of the NIS2 Directive is to increase the cybersecurity maturity of European entities transversally, filling gaps and avoiding disparities between the Member States of the European Union. Member States should join the EU's efforts to strengthen the resilience of cybersecurity networks and not undermine those efforts by adopting a selective approach, or by adding additional measures that are not established, restricting trade in the Single Market. Relevant sectors have been identified under NIS2 to a large extent at EU level, including among others digital infrastructure, energy, transport, health and manufacturing sectors. Any extension, misalignment or fragmentation of this scope should be avoided during the transposition into national law. In addition, a clear and harmonised scope will ensure a more predictable and consistent implementation of the cybersecurity legal framework and will result in enhanced security as a whole.

The lack of automation and innovation in regulatory processes further complicates efforts to streamline compliance and maintain consistency across borders. As a result, organizations face a complex and fragmented environment, increasing the challenges of managing cybersecurity across borders efficiently.

IMPLEMENTATION

The implementation of cybersecurity regulations, such as the NIS2 Directive, faces difficulties, mainly because of the inconsistent regulatory interpretations and timelines across member states. 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. For example, there is a lack of a central system for monitoring compliance and regulation transposition.

As of November 28, 2024, Croatia, Italy, Belgium and Lithuania are the only countries that fully transported NIS2 based on the infringement procedure started by the EC leaving business operating across borders to navigate inconsistent legal frameworks. Moreover, in the case of many countries, there is a lack of publicly available information regarding the status of implementation, conformity and compliance, NIS2 security requirements, frameworks, and risk management.

Overall, many organizations face significant challenges in meeting cybersecurity regulations due to several factors. There is widespread uncertainty about which entities are covered by these regulations and the specific requirements they must fulfill. This is further compounded by the high costs of certification and compliance, which disproportionately impact small and medium-sized enterprises (SMEs). Many companies also lack experience in adopting foundational principles such as „security by design" and „security by default," leaving them ill-equipped to address regulatory demands effectively. Additionally, limited access to cybersecurity experts and the absence of clear composition standards, particularly within supply chains, exacerbate the problem. These issues are further magnified by persistent difficulties in areas like documentation, risk assessment, and security testing, all of which are critical for achieving compliance.

ADMINISTRATIVE AND REPORTING ISSUES

Complicated administrative processes and inconsistent incident reporting obligations present significant challenges to the effective implementation of legislative solutions. Security questionnaires, intended to assist businesses, often consist of hundreds of detailed questions, making them time-consuming and burdensome for employees. Additionally, answering such surveys can be costly for respondents. Notifying incidents to multiple authorities is another major source of complexity, as noted by numerous survey respondents (ECSO). The absence of a unified system, platform, or entity for reporting incidents increases the risk of duplication. Determining the appropriate authority for reporting depends on factors such as the business's industry, the specific directive or act, and national law. This complexity is further amplified when a business operates in multiple industry categories.

The interplay between NIS2 and sector-specific legislation, such as the Digital Operational Resilience Act (DORA), serves as a clear example. The European Commission has clarified that for financial firms within the scope of DORA, which may also overlap with NIS2, DORA's requirements take precedence. However, this clarity does not extend to ICT third-party providers designated as critical third-party providers (CTPPs). These providers fall under the direct oversight of the European Supervisory Authorities (ESAs), requiring compliance with ongoing information requests and recommendations from the ESAs, while simultaneously adhering to reporting obligations under NIS2. This dual compliance requirement conflicts with the Commission's "once only" policy, introducing additional complexities without a clearly defined benefit to security or resilience, even as the Commission aims for regulatory simplification.

Different directives and legislative frameworks demand varying types of information. For instance, NIS2 imposes stricter obligations for incident reporting. The differing definitions and thresholds for reportable incidents across countries, with some requiring reporting beyond significant incidents and others applying inconsistent cross-border impact criteria, force companies to expand their monitoring capabilities and adopt country-specific incident response procedures. This increases resource demands and heightens compliance risks (ECSO). Furthermore, the timelines for reporting incidents under different directives and laws vary significantly, complicating compliance efforts and further burdening organizations. Additionally, there is often no explicitly defined threshold for what constitutes a disruption or incident. Criteria for defining incidents or disruptions differ across regulations, ranging from vague descriptions, such as those in NIS2, to specific requirements like duration, geographical data, or economic impact, as stipulated in DORA. These inconsistencies not only increase the administrative burden on organizations but also raise the likelihood of unintentional errors in reporting.

POLICY AND STRATEGY

The growing number of regulations creates difficulties in managing compliance. This highlights the need to develop a comprehensive European industrial strategy for cybersecurity that can streamline regulatory efforts and promote cohesion. Greater involvement of both public and private stakeholders in the decision-making process is essential to ensure that regulations are practical and aligned with the challenges of the rapidly evolving cybersecurity landscape.

Additionally, there is a lack of dialogue between regulators and companies, leading to low awareness of requirements and a high political complexity of negotiations and differences in member states' approaches.

Other practical challenges exist in the newly adopted framework, with often opposing political choices made in regulations addressing cybersecurity risks. For example, NIS2 does not include mandatory vulnerability reporting but instead focuses on reporting of significant incidents, which is further clarified also in the Implementing Act (Commission Implementing Regulation on critical entities and networks) from 17.10. 2024. However, there is a concern that sharing information about vulnerabilities across various authorities could increase security risks. The same contradictory approach is foreseen under the Cyber Resilience Act (CRA), which requires reporting of actively exploited vulnerabilities. Despite the support among experts about maintaining a vast and open vulnerability reporting system, the EU has only recognized this risk partially (in NIS2). This can give rise to new threats and will need careful management by ENISA and national authorities to prevent this policy from backfiring. More generally, it points to the need for a more coherent regulatory vision about how to best address cybersecurity risks, particularly in a coordinated manner across the Union (and with global partners). With DORA applying as of 17 January 2025, the potential insecure circulation of vulnerabilities amongst authorities, which would introduce further attack vectors, requires urgent attention from policy makers and regulators to protect the cybersecurity of the Union.

Looking ahead, the need for stakeholders to prepare and adapt to the new cybersecurity requirements will not abate. This does not include the practical difficulties caused by the delayed implementation of the NIS2 Directive across the Member States. The forthcoming application of the CRA is a clear example, but other measures such as the development of certification schemes for managed security services and application of the new EU Digital Wallet (eIDAS regulation) will introduce further compliance work. Within the CRA, there are many secondary acts to be adopted to clarify e.g. the reporting obligations (Art. 14), specifications for critical products with digital elements, technical description of important products with digital elements, and presumption of conformity (Art. 27), among others. Where these differ from existing regulatory frameworks, often as mandated by the Act itself, or from international standards and best practice, this will only add to the regulatory burden facing companies and the complexities encountered by responsible authorities.

IMPACT ON SMEs

Small and medium-sized enterprises (SMEs) face unique challenges in implementing legislative solutions. One of the most pressing challenges is limited resources, both human and financial. These enterprises operate with a smaller work force and a smaller budget in comparison to big businesses. Keeping up with ever-changing legislation requires time, expertise, and a lot of documentation and reporting, which can be hard for SMEs employees as they are often required to handle multiple tasks and do not have the time to take on additional workload. This might lead to delayed compliance or unintentional violations. Moreover, due to the small budgets, SMEs may not have the financial ability to hire external experts to help with the implementation process or to fulfill roles which would be created as a result of implementing the new legislation, which can further increase the likelihood of unintentional violations. Furthermore, some legislation might require the purchase or adaptation of a more advanced and expensive technology, which might simply be out of the budget for some SMEs. A lack of support and guidance can also stand as a major obstacle to implementing legislative changes. A lack of tailored support from the government industry bodies can make implementation extremely difficult and confusing, especially if not equipped with the proper expertise.

SUPPLY CHAIN CHALLENGES

The global nature of modern supply chains creates inherent security challenges due to varying legal requirements. Suppliers from various regions must navigate through regulations and compliance standards, often resulting in gaps in security. Some regions enforce stringent cybersecurity and data protection laws, while others operate under weaker or outdated frameworks, creating vulnerabilities that malicious actors can exploit. These inconsistencies jeopardize the integrity of supply chains and are further exacerbated by geopolitical tensions, such as trade restrictions or sanctions, which introduce operational uncertainty and complicate compliance requirements.

The lack of harmonized certification standards further amplifies these challenges. Suppliers frequently face the burden of adhering to multiple, sometimes conflicting, frameworks or region-specific regulations. This fragmented approach not only increases compliance costs but also makes it difficult for organizations to assess their suppliers' security postures. Certifications recognized in one jurisdiction may not align with or be accepted in another, leaving gaps in protection. As a result, organizations struggle to implement

comprehensive risk management strategies across the supply chain.

Tracking and addressing vulnerabilities is also hindered by the fragmented information systems used by suppliers. Some rely on more advanced information systems, while others may rely on less mature ones which may lead to delays and errors. Many rely on disparate data management systems, ranging from advanced automated platforms to outdated manual processes, leading to delays, errors, and blind spots. This lack of standardization makes it difficult to compile and analyze critical security information effectively. The problem is compounded by the cross-border nature of supply chains, where components or services often originate from third- or fourth-tier suppliers. This complexity makes it challenging to trace the origins of vulnerabilities, leaving organizations exposed to risks that may cascade throughout the supply chain.

RECOMMENDATIONS

STANDARIZATON AND HARMONIZATION OF REGULATIONS

1. The NIS2 Directive should be transposed without national additions, contributing to the harmonisation of the Member States. This approach is in line with several external research projects that suggest that the open economy and a focus on a set of security requirements could enhance global security while promoting healthy competition in the market.

2. The policy need is twofold: consolidation around the core set of procedures, rules and the one-stop shop mechanism introduced in the NIS2 regime; and harmonization provisions preventing Member States from deviating from this regulatory baseline. This could include a specification, that would clarify, that if already a directly applicable legal instrument of the European Union exists, which imposes on critical (essential) infrastructure entities obligations in the area of ensuring the resilience of critical infrastructure entities and these obligations have at least a comparable effect to the obligations imposed on critical infrastructure entities pursuant to the CER, the provisions of CER governing the obligations to introduce and implement measures to strengthen resilience and report incidents do not apply to these authorities and persons, including provisions on the supervision of compliance with the aforementioned obligations.

3. Create comprehensive horizontal interpretative guidelines that provide clear insights for implementation. These guidelines should include detailed Q&A sections to address common concerns and vagueness. Additionally, they should emphasize and promote a risk-based approach.

4. Develop and establish a set of minimum European security requirements, formalized through the use of standardized questionnaire templates.

5. Find a balance between being specific and generic in terms of control measures. Being too specific can lead to inconsistencies between cyber regulations, while relying on market-leading standards allows for broader interpretation. However, basing regulations on international standards can facilitate alignment between organizations and ensure long-term adaptability.

6. Security incident reporting requirements vary across regulations, with some differences being non-fundamental but still contributing to increased complexity. It is recommended to align these requirements within EU cybersecurity regulations wherever justified, to streamline compliance and reduce unnecessary complexity.

REGULATORY ASSESSMENT PROCEDURES

1. Introduce a procedure to systematically assess the impact of cybersecurity regulations on competitiveness and companies' ability to safeguard Europe's key assets prior to their implementation. This proactive legislative review process would ensure that new regulations strike a balance between enhancing security and maintaining economic vitality, fostering innovation, and supporting the strategic interests of the region.

2. Reducing administrative burdens by simplifying processes and reporting is needed. We recommend preparing a detailed guide on all regulatory requirements stemming from the horizontal and sectoral legislation in the area of cybersecurity, including (but not exclusively) sectoral initiatives affecting FSI, energy and automotive. This guide should provide (a) policymakers with an understanding of the current state of EU cybersecurity regulations, to inform further regulatory works; and (b) regulated entities, including businesses operating in Europe, with clear overview on the application of the rules, including deadlines and processes to follow where regulatory clauses conflict. It should also stand as a roadmap for simplification and deletion of contradictory rules, while also identifying best practices that support the ultimate objective of enhancing the security of the EU. NIS2 provides for clear timelines and requirements on incident reporting, and in order to streamline and simplify the entire reporting system within the EU, NIS2 structure and logics on reporting should be as much as possible a guiding element also for sectoral reporting rules. We would advise that future revisions of cross-sectoral or sectoral requirements (i.e. DORA 2) area are aligned in order to facilitate compliance. As mentioned above, for the sake of legal clarity, we would encourage the EU policy makers to ensure that the main principles of the NIS2 Directive, including the system on reporting and one stop shop rules incorporated within it, effectively applies across all industries.

3. DORA and other regulations are going to increase the pressure on entities delivering ICT services to disclose information and subject themselves to audit from clients. With this potentially driving the cost of service up, it would be desirable to consider guidance for third party assurance for regulations such as DORA or NIS2. An additional factor

supporting this is the fact that some of the client--vendor relationships may be between competitors thus introducing a third party may resolve a challenge related to sharing information which could lead to losing competitive advantage.

IMPROVING COOPERATION AND DIALOGUE

1. Encourage the organization of more cross-sector dialogues between policymakers and industry stakeholders to better integrate companies' needs and technical expertise into the legislative process. These dialogues would foster collaboration, ensure regulations are practical and effective, and promote a shared understanding of challenges and opportunities in cybersecurity across sectors.

2. Promote cross-border collaboration by enhancing stakeholder involvement in EU-level decision-making processes. This approach would ensure a more inclusive and representative framework, fostering alignment across member states, integrating diverse perspectives, and strengthening the collective ability to address cybersecurity challenges at a European level.

3. As a way to protect the rights of companies and balance their security and development, it is recommended that the views of the sector be fully heard in the formulation and implementation of these standards:

   3a. Establish a mechanism to welcome the views of the business sector and industry associations; and create channels through which companies can expose their position.

   3b. To select the focus of these opinions in a pertinent way. If the impact of these standards on different companies and sectors is different, it will also be relevant to listen to the positions of the various companies representing the sector, industry associations and chambers of commerce.

   3c. Carefully analyse and study the opinions and suggestions put forward by companies, industry associations and chambers of commerce, fully consider their interests and the impact of interests on other relevant companies and industries, and welcome and adopt relevant and reasoned opinions.

4. Establish a cybersecurity advisory body, with members from relevant government departments, carriers, suppliers and industry associations, to provide professional advice to regulators.

OPTIMIZING COMPLIANCE PROCESSES AND CERTIFICATION

1. Embrace automation by leveraging advanced technologies, such as artificial intelligence and machine learning, to enhance the efficiency and accuracy of managing regulatory requirements, streamlining reporting processes, and monitoring compliance. These technologies can help organizations automatically track changes in regulations, generate timely and accurate reports, and identify potential compliance risks in real time.

2. The use of standardised certification frameworks is recommended to help eliminate market fragmentation, simplify rules and improve efficiency in cybersecurity management. The use of uniform certification standards can simplify the rules to improve efficiency in the implementation of cybersecurity management, reduce costs for industry and companies in the product certification process, accelerate access to and use of advanced products and technologies, and accelerate the digital transformation of industry.

3. A clear guidance on conducting comprehensive supply chain risk assessments (SCRAs) of potential risks is crucial. Standardizing the assessment process facilitates the identification of risks, optimizes decision-making, and promotes the continuous improvement of supply chain cybersecurity. By working collaboratively with suppliers to implement sound cybersecurity practices, organizations are able to mitigate risks and ensure the smooth functioning of their supply chains. Research by the European Union Agency for Cybersecurity (ENISA) shows that compliance with the ISO set of standards (ISO 27001/27002/28000/31000, etc.) can be effective in ensuring supply chain security.

BUILDING RESOURCES AND AWARNESS

1. Training and education should be emphasized and considered as a priority. Supporting companies, especially SMEs, in gaining the knowledge and skills is necessary to implement requirements such as „security by design".

2. It is recommended to provide guidance on how to apply the regulation to small companies, as it has been noted that regulations are often designed with large corporations in mind. Some countries, for example, support NIS2 by implementing a tiered approach. Basing requirements on company size

or maturity could help optimize compliance costs, which can be a significant burden for some organizations. This approach may, in turn, encourage broader adoption of effective security measures. Some countries seem to support that for e.g. NIS2 through implementation of tiers. Such an approach based on company size or maturity may also help optimize the cost of compliance, which to some may be a significant burden. This may de facto increase adoption of true security measures.

3. Establish a centralized information hub dedicated to regulations, such as NIS2, to offer companies a single, reliable source for accessing the latest data on timelines, requirements, and compliance guidelines. This hub would provide clear, up-to-date, and easily navigable information, ensuring businesses of all sizes can stay informed and prepared for regulatory changes.

IMPROVEMENTS IN REPORTING AND MONITORING

1. Establish a centralized process by designating a single point of contact for reporting all cybersecurity incidents, extending beyond the requirements of NIS2. This approach will ensure clarity, consistency, and efficiency in incident management.

2. Implement standardized root cause templates and data formats, particularly for incident reporting, with clear and precise definitions to facilitate international communication and problem-solving. Establish an automated “one-stop shop” system for submitting reports and distributing information, ensuring alignment with various regulatory requirements. This approach would streamline processes, enhance consistency, and improve the efficiency of information sharing across borders and sectors.

3. Implement standardized templates and data formats, particularly for incident reporting, with clear and precise definitions to facilitate international communication and problem solving. An automated “one-stop shop” system for submitting reports and distributing information in line with various regulatory requirements is called for.

4. Recommend the introduction of unified European templates for security questionnaires to minimize effort and administrative burden. These templates should be designed to allow up to 75% of questions to be pre-filled with the help of AI, which streamlines the process for organizations while ensuring consistency and compliance across member states. This approach would save time, reduce duplication, and enhance the efficiency of security assessments at the European level.

5. Including more specifics about the information required for the incident report. For NIS2, for instance, the progress report does not have any requirements listed. What one doesn’t deem important, another might, and hence this will save more time as the authorities will not have to contact entities to provide basic details. The same should be applied to any type of report which is required by the directive / law. These requirements should be synchronized in order to make the process easier for the parties involved. Providing contact details should be essential and clearly stated in the requirement for each report.

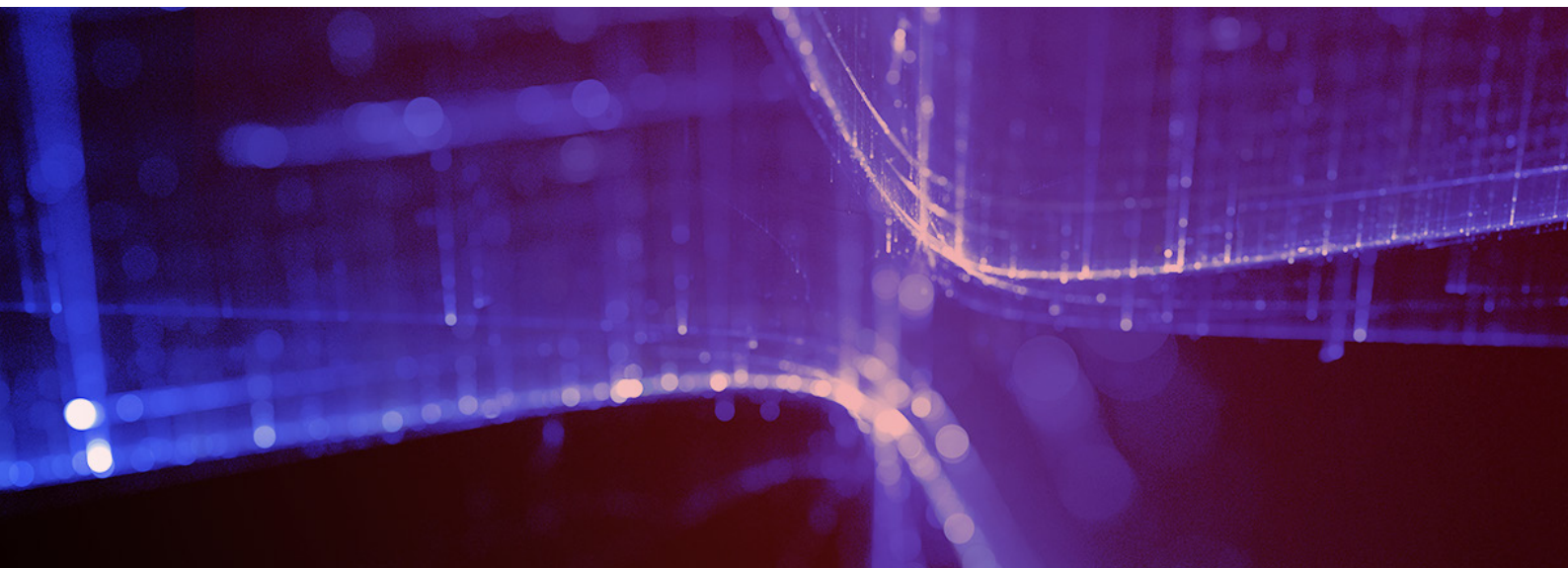
6. The conditions under which the public should be notified should be unified and the manner in which the public is notified should be established as well. There is no timeline given for reporting to the public, and it might be beneficial to create a unified timeline.

7. It is recommended to consider creating a common name for the incident reporting. Different directives/laws tend to use different phrases for the report, it might be helpful to utilize one phrasing when dealing with cybersecurity incident reports.

Summary of key recommendations

Discussions like these are essential to uncover the root of the problem and identify practical solutions. By fostering dialogue among policymakers, businesses, and other stakeholders, it becomes possible to gain a deeper understanding of the challenges and pinpoint areas for improvement. The survey conducted presented the greatest compliance challenges for organizations. The presented challenges in implementing EU cybersecurity regulations highlight the need for clearer and more coordinated frameworks. Currently, organizations face overlapping rules, inconsistent interpretations across member states, and heavy administrative demands, which make compliance particularly difficult for smaller businesses with limited resources. This complexity creates confusion, adds costs, and detracts from effective cybersecurity measures.

To tackle these issues, there is a need to simplify processes, improve collaboration among stakeholders, and ensure national approaches align with EU-wide objectives. Regulations should be practical, flexible, and consistent, helping organizations meet their obligations without unnecessary strain. By improving coordination between governments, businesses, and other stakeholders, the EU can build stronger cybersecurity resilience, support innovation, and ease the compliance burden. These efforts will contribute to a safer digital environment, better equipped to handle emerging cyber threats, while enabling businesses to thrive and innovate.



Deloitte.

Challenges of the NIS2 Directive

The NIS2 Directive, which aims to increase the level of security of network and information systems in the European Union, poses new challenges for organizations. These include both the adaptation of existing processes and the implementation of new technical, legal and organizational solutions. Failure to comply with the requirements may result in high financial penalties and damage to the company's reputation. Therefore, it is worth taking action now to ensure compliance with the new regulations.

Key challenges of the NIS2 Directive

1. Security Gap Analysis: Organizations must conduct a comprehensive assessment of current systems and processes to identify areas for improvement.

2. Implementation of new requirements: The implementation of technical safeguards, such as threat detection systems or incident management, requires time, resources and appropriate know-how.

3. Legal compliance: The directive imposes the obligation to meet certain formal requirements, such as incident reporting or risk management.

4. Maintaining Compliance: Organizations must constantly monitor their systems and adapt procedures to changing legal and technological requirements.

How can Deloitte help?

Deloitte specializes in comprehensive support for organizations in the process of meeting the requirements of the NIS2 directive. Our services include:

1. Gap analysis:

- We conduct detailed audits, identifying areas where the organization does not meet NIS2 requirements.
- We prepare a report with recommendations, indicating specific steps to take.

2. Requirements Implementation:

- We help you implement appropriate technical measures, such as information security management systems (ISMS), and processes in accordance with best practices.
- We support the development and implementation of business continuity plans and incident response strategies.

3. Legal and organizational consulting:

- We cooperate with legal experts to ensure full formal and legal compliance.
- We advise on risk management and creating a safety culture in the organization.

4. Maintaining Compliance:

- We offer monitoring, training and process update services to ensure long-term compliance with the Directive.

Why is it worth acting now?

The NIS2 directive imposes strict deadlines for implementing the requirements, and the process of adapting the organization is time-consuming. Starting action now allows you to avoid rushing, minimize the risk of fines, and build a solid foundation for digital security.

Take action today! Contact Deloitte for a free consultation and to find out how we can help your organization meet the requirements of the NIS2 directive.