

4 JUNE 2025

Digital simplification package: Our cyber recommendations

The surge of cybersecurity legislation in recent years has been necessary and justified. Most notably, NIS2 and the Cyber Resilience Act (CRA) mark a decisive step in strengthening Europe's cyber defences and ensuring shared responsibility across the value chain.¹ But ambition has come at the cost of coherence, placing disproportionate burdens on companies without necessarily improving security outcomes. The digital package offers a pragmatic opportunity to address these growing pains.²

Table of contents

Establish a unified reporting framework	2
Unify incident thresholds	3
Standardise 72-hour timeline	3
Adopt a common reporting template	3
Create a reporting one-stop shop	4
Align national contacts	5
Recognise NIS2 audits across borders	5
Establish an EU-wide coordinated vulnerability policy	6
Make CRA obligations more manageable	7
Apply only when harmonised standards are available	8
Support self-assessment as a transition for important products	8
Limit reporting to the support period	9
Allow RED-compliant products a CRA transition period	9
Tailor requirements for industrial systems	9
Clarify spare parts exemptions	10
Accept compensating countermeasures	10

¹ Directive (EU) 2022/2555 and Regulation (EU) 2024/2847, respectively.

² These recommendations should be read in conjunction with our existing positions on the Cybersecurity Act review, available at https://cdn.digitaleurope.org/uploads/2023/09/DIGITALEUROPE_Adapting-ENISAs-mandate-and-collaboration-in-a-changing-cyber-landscape.pdf, and on the issues to be clarified in the interpretation and application of the CRA, available at https://cdn.digitaleurope.org/uploads/2024/09/Developing-guidelines-for-the-Cyber-Resilience-Act_DE.pdf.



Exclude inherently low-risk products.....10

Establish a unified reporting framework

- ▶▶ Introduce a harmonised threshold for reporting of significant incidents, based on NIS2.
- ▶▶ Align incident reporting timelines with the 72-hour GDPR model to allow a thorough initial assessment before notification, removing premature early warnings.
- ▶▶ Create a single, harmonised reporting template applicable under NIS2, the CRA, the GDPR and other laws.

Europe has a multiplicity of reporting obligations stemming from various regulations, primarily NIS2, the CRA and the General Data Protection Regulation (GDPR).³ Each introduces its own definitions, reporting thresholds, timelines and content requirements applying effectively to the same incident, which may need to be reported multiple times under these different rules. The following table provides a summary overview:

Regulation	Trigger	Timeline	Content	Authority	Platform
Cyber Resilience Act (CRA)	Actively exploited vulnerabilities and severe incidents	<ul style="list-style-type: none"> - Early warning: within 24 hours of becoming aware - Incident notification: within 72 hours - Final report: within 14 days after implementing corrective measures (for vulnerabilities) or within 1 month after the incident notification (for severe incidents) 	<ul style="list-style-type: none"> - Technical description - Affected products - Impact assessment - Mitigation measures 	National Cyber Security Incident Response Team (CSIRT) and ENISA	Single reporting platform coordinated by ENISA
NIS2 Directive	Significant incidents affecting essential and important entities	<ul style="list-style-type: none"> - Early warning: within 24 hours - Incident notification: within 72 hours - Final report: within 1 month 	<ul style="list-style-type: none"> - Initial facts - Incident nature - Impact assessment - Mitigation measures 	Relevant CSIRT or competent national authority	National CSIRT portals, coordinated by ENISA
General Data Protection Regulation (GDPR)	Personal data breaches posing high risk to individuals	Without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach	<ul style="list-style-type: none"> - Nature of the breach - Categories and number of data subjects and records concerned - Likely consequences - Measures taken or proposed 	Competent data protection authority	National data protection authority's reporting system

To address this fragmentation, the digital package should align key aspects whilst respecting each law's specific objectives.⁴

³ Regulation (EU) 2016/679.

⁴ This paper primarily refers to NIS2 and the CRA as horizontal cybersecurity frameworks. Sector-specific instruments also apply, notably Regulation (EU) 2022/2554 (DORA) for the financial sector and Regulation (EU) 2025/327 (European Health Data Space) for health data infrastructure. Directive (EU) 2022/2557 (CER) complements NIS2 by addressing non-cyber operational risks (e.g. physical attacks, natural disasters). As many entities fall under multiple frameworks simultaneously, the paper's recommendations on streamlining cybersecurity reporting – including timelines, formats and channels – are equally relevant to these laws.



Unify incident thresholds

The digital package should introduce a **harmonised threshold for when an incident is significant enough to be reported**. This threshold would maintain consistency whilst allowing each regulation to interpret it within its context. The most suitable baseline is the NIS2 concept of a significant incident, characterised by severe operational disruption or considerable damage.⁵

Standardise 72-hour timeline

Timelines are a critical element in reporting, as they determine how quickly companies must notify authorities after becoming aware of an incident. It is important to distinguish between the operational response to an incident, e.g. containment and mitigation, and the separate obligation to inform competent authorities. Whilst companies typically react immediately to address and contain incidents, notifying authorities is a separate process that should follow a reasonable assessment of the situation.

Both the CRA and NIS2 currently require an early warning within 24 hours of awareness, pushing companies to submit speculative or incomplete information. In addition, DORA stipulates a four-hour deadline for financial entities' initial notifications.⁶ However, these laws also provide for a more detailed notification within 72 hours, a model that mirrors the more flexible standard found in the GDPR: 'without undue delay and, where feasible, not later than 72 hours after becoming aware.'⁷

This 72-hour model allows organisations sufficient time to verify the incident, assess its impact and gather essential details. The digital package should therefore **establish a harmonised timeline based on the 72-hour model, eliminating the need for premature early warnings** and promoting higher-quality incident reporting.⁸

Adopt a common reporting template

The Commission already has the power to adopt implementing acts to establish reporting templates under both NIS2 and CRA.⁹ However, these templates remain distinct and developed independently. Furthermore, they are not valid under other frameworks.


⁵ Importantly, DORA already establishes a categorisation system for ICT-related incidents to qualify as material, based on predefined thresholds such as the number of customers affected, the impact on critical services and the duration of the disruption.

⁶ Delegated Regulation (EU) 2025/301.

⁷ The digital package should also establish a common understanding of 'becoming aware,' consistent with EDPB Guidelines 9/2022, as well as Commission Implementing Regulation (EU) 2024/2690. This means that after being informed of a potential issue, entities may undertake a short investigation period to confirm whether a breach has occurred. During this investigation phase, the entity is not regarded as being aware of the breach. This ensures companies are not forced to report incidents prematurely, whilst still maintaining prompt notification once the incident is reasonably confirmed.

⁸ NIS2, the CRA and DORA also require a final report for incidents one month after notification, which serves a distinct purpose and is not paralleled in the GDPR. We do not propose extending this requirement to other frameworks, but acknowledge its role in follow-up reporting where it already applies. This recommendation concerns incident notifications only; separate provisions exist under the CRA for the reporting of actively exploited vulnerabilities, which we address in the 'Establish an EU-wide coordinated vulnerability policy' section below.

⁹ Arts 23(11) NIS2 and 14(10) CRA.



The digital package should address this by mandating a **single, harmonised reporting template that can be adopted under both NIS2 and CRA and is valid across other regulations** like DORA and the GDPR. This would prevent the creation of divergent templates and significantly reduce the compliance burden for companies, which currently face the challenge of adapting incident reports to meet multiple legal requirements.

The harmonised template should include the following core elements, applicable across all relevant regulations:


- » Incident description: Clearly define the nature and context of the incident, specifying whether it involves a cybersecurity breach or a personal data breach.
- » Impact assessment: Provide an evaluation of the degree of disruption or harm caused, aligned with the harmonized threshold established for significant incidents.
- » Mitigation measures: Describe the steps taken to address or contain the issue, including technical and procedural responses.
- » Follow-up actions: Outline any ongoing or planned measures to prevent recurrence.
- » Additional fields: Include optional fields to accommodate specific requirements under NIS2, the CRA, the GDPR and DORA.

To avoid unnecessary overlap and maintain regulatory clarity, the digital package should respect DORA's sector-specific role for the financial sector. It should, at the same time, facilitate compliance by allowing financial entities and ICT providers to use the single harmonised reporting template proposed for NIS2 and CRA to also meet DORA requirements. This approach would reduce double reporting and support the ongoing development of the creation of a Single EU Hub for incident reporting envisaged under DORA,¹⁰ whilst ensuring that financial entities are not subjected to conflicting reporting obligations.

Create a reporting one-stop shop

- » Strengthen the new single reporting platform managed by ENISA to cover all relevant regulations, with automatic routing to national authorities.
 - » Mandate that Member States designate the same entity (preferably the national CSIRT) as both the CRA electronic notification endpoint and the NIS2 single point of contact.
 - » Set a mutual recognition policy requiring Member States to accept NIS2 compliance audits carried out under another country's national framework.

¹⁰ The European Supervisory Authorities (ESAs) have jointly developed a report on the feasibility of further centralising major ICT-related incident reporting through the establishment of a single EU Hub, as mandated by Art. 21 DORA. The report is available at https://www.esma.europa.eu/sites/default/files/2025-01/JC_2024_108_Report_on_the_feasibility_for_further_Centralisation_of_reporting_of_major_ICT_incidents.pdf.



One of the key challenges in incident reporting is the complexity arising from the multiplicity of competent authorities. Different regulations mandate reporting to different authorities, often without clear coordination.

The digital package should build on the **single reporting platform** that has already been set up under the CRA. This platform, managed by ENISA, **should be strengthened to serve as a unified entry point**.¹¹

The platform should respect Member States' competence by automatically routing information to the relevant national authorities, preserving their existing prerogatives.

Consolidating incident reporting through the single platform would significantly reduce the administrative burden on companies and foster greater coordination of cyber responses and capabilities. An enhanced platform would strengthen ENISA's role whilst safeguarding national competences.¹²

Align national contacts

Under the CRA, Member States are required to designate electronic notification endpoints to facilitate incident reporting through the single reporting platform managed by ENISA. Similarly, NIS2 mandates each Member State to designate a single point of contact responsible for cross-border cooperation and communication with other Member States and ENISA.

Whilst the CRA and NIS2 do not explicitly require that the same entity serve both roles, there is no legal impediment to such an alignment. In fact, aligning these roles can streamline incident reporting processes, reduce administrative burdens and enhance coordination between national and EU-level cybersecurity efforts.


For these reasons, the digital package should recommend that **Member States designate the same entity, preferably the national CSIRT, as both the electronic notification endpoint under the CRA and the SPOC under NIS2**. This alignment would simplify reporting processes for entities subject to both regulations, ensure consistent communication channels between national authorities and ENISA, and enhance the efficiency of incident response and coordination efforts.

Recognise NIS2 audits across borders

The fragmentation of NIS2 compliance audits across Member States creates significant challenges for companies operating in multiple jurisdictions. Due to the national transposition of NIS2, companies often face 27 separate sets of requirements, despite the core obligations stemming from the same directive. This inconsistency results in the same centralised cybersecurity processes being audited multiple times across different countries, significantly increasing administrative burdens and compliance costs.

¹¹ This could include not only the CRA but also NIS2, the GDPR and other relevant laws.

¹² Until the single reporting platform is fully operational, ENISA could establish an interim dashboard listing each Member State's designated contacts. This would enhance the accessibility of current reporting channels. In some cases, national authorities may submit follow-up questions to entities after an incident report. With appropriate technical capabilities, the CRA single reporting platform could allow entities to share answers provided to one authority with others, thus potentially reducing duplicative inquiries.



An illustrative example is Belgium's CyberFundamentals (CyFun®) Framework, a national certification scheme designed to assess compliance with NIS2 requirements.¹³ Whilst CyFun® is recognised by the Centre for Cybersecurity Belgium (CCB), other Member States may not automatically accept it, despite its rigorous standards. The existence of such national certifications highlights the need for a mutual recognition policy that would prevent duplication and foster a more integrated approach to NIS2 compliance.

To address this issue, the digital package should directly **set a mutual recognition policy for NIS2 compliance audits**. This policy should require Member States to accept audits conducted under another country's NIS2 transposition law. This will help companies comply more efficiently in a multi-jurisdictional environment.¹⁴

Establish an EU-wide coordinated vulnerability policy

- ▶▶ Establish a unified coordinated vulnerability disclosure process that integrates the single reporting platform and the European vulnerability database managed by ENISA.
- ▶▶ Remove the obligation to report actively exploited, unpatched vulnerabilities, which could expose attack vectors and pose significant security risks.

Handling vulnerabilities correctly is crucial to balancing security and transparency. The digital package should move away from the current scattered approach and establish a common, coordinated vulnerability disclosure (CVD) policy at the EU level.

The EU already has the essential tools in place to manage vulnerability reporting. NIS2 established the European vulnerability database, managed by ENISA, for the voluntary disclosure of publicly known vulnerabilities. The CRA created a single reporting platform, where manufacturers report actively exploited vulnerabilities and severe incidents to ENISA and national CSIRTs.

Although these mechanisms were developed at different times and under separate legislative instruments, they are inherently complementary. These tools should be more closely linked to ensure that they function as a unified process.

The current CVD framework is primarily mandated at the Member State level under NIS2. Whilst ENISA is responsible for the European vulnerability database, the overall coordination of CVD at the EU level remains limited. The CRA introduces manufacturer-level obligations, but does not by itself create a full EU-wide policy or process for coordinated disclosure involving all relevant actors (e.g. ENISA, CSIRTs, independent researchers and cross-border coordination mechanisms).¹⁵

¹³ <https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework>.

¹⁴ CyFun® could be submitted to the European co-operation for Accreditation (EA) for broader recognition across Member States. Whilst EA accreditation would facilitate mutual acceptance of the certification results, it would not automatically ensure that Member States recognise it as fulfilling NIS2 compliance requirements. Therefore, a mutual recognition policy set by the digital package remains necessary to guarantee uniform acceptance across the EU.

¹⁵ Annex I, Part II CRA.

The digital package should leverage the existing tools to **establish a unified EU CVD process** that aligns with international standards and industry practices.¹⁶ The single reporting platform should be the central entry point for submitting vulnerabilities, with all reports feeding into the European vulnerability database. Strengthening ENISA's role as the central coordinator, whilst preserving the national responsibilities of CSIRTs, will improve efficiency and alignment across the EU.

At the same time, importantly, **the reporting of 'actively exploited' vulnerabilities, for which mitigation is not yet available, should be removed.**¹⁷ Reporting unpatched vulnerabilities creates significant cybersecurity risks by potentially exposing attack vectors. Both industry and consumer organisations have strongly cautioned against this approach, as it contradicts best practices in vulnerability handling and disclosure.¹⁸

Make CRA obligations more manageable

- ▶▶ Delay the application of CRA essential requirements until 12 months after relevant harmonised standards for Annex I are published.
- ▶▶ Allow companies to self-assess important products until harmonised standards for these products are available and notified bodies in place.
- ▶▶ Limit reporting obligations to products' declared support period, avoiding burdens linked to obsolete or unsupported systems.
- ▶▶ Introduce a three-year transition period under which products already compliant with Radio Equipment Directive (RED) cybersecurity rules are automatically considered compliant with the CRA.
- ▶▶ Adapt CRA rules for industrial systems by clarifying that the spare parts exemption covers full product replacements and software tools, and by allowing alternative security solutions where full compliance is not technically feasible.
- ▶▶ Exclude simple, low-risk products – like toothbrushes and basic sensors – that do not pose real cybersecurity threats.

¹⁶ Notably, ISO/IEC 29147 for vulnerability disclosure and ISO/IEC 30111 for vulnerability handling, reflecting Recital 58 NIS2. The Common Vulnerabilities and Exposures (CVE) programme is the global standard for publicly disclosing vulnerabilities. The EU vulnerability database should align with it by including a field for CVE identifiers and enabling requests for ENISA – acting as a CVE Numbering Authority – to assign a CVE ID when none exists. ENISA already imports CVE data into the EU database.

¹⁷ Art. 14(1) CRA.

¹⁸ Importantly, in this context, the requirement under Art. 13(6) CRA for manufacturers to report vulnerabilities found in third-party components, including open source, and to share remediation code should not be regulated in isolation. This type of supply chain coordination is better addressed through a structured EU-wide CVD policy under the digital package, where roles, safeguards and communication protocols can be clearly defined and aligned with international best practice.

Apply only when harmonised standards are available

The CRA and other NLF-based legislation rest on compliance through harmonised standards, developed or adopted by European standards bodies and published in the Official Journal of the EU (OJEU). Whilst it is well understood that international standards – like ISO/IEC 27001 or IEC 62443 – can be a basis for harmonised standards, they cannot be automatically recognised for compliance, as harmonised standards must align specifically with the essential requirements outlined in the CRA. The process of recognising harmonised standards is driven by how the Commission assesses outputs from European standards bodies.

Creating harmonised standards can take a significant amount of time, especially when they must differ from existing international standards to meet specific European essential requirements. On average, it takes four years to develop a complete set of harmonised standards, including the necessary consultations, technical adjustments and formal adoption. This lengthy process means that compliance obligations should not be enforced before the standards are finalised and published.¹⁹

To address this gap between legislative expectations and practical realities, the digital package should set a clear rule that **manufacturer obligations should become applicable no earlier than 12 months after the related horizontal harmonised standards are published** in the OJEU.²⁰ This approach provides companies with predictability and adequate time to adapt.

Support self-assessment as a transition for important products

The CRA mandates EU-type examination procedure (Module B) for important products with digital elements that do not fully conform to harmonised standards.²¹ This requires both the submission of technical documentation and the physical testing of a specimen by a notified body. This approach diverges from the more proportionate procedure under frameworks such as the RED, where conformity is typically demonstrated through design-type examination without mandatory physical testing for each product type.


In practice, manufacturers and third-party laboratories already carry out extensive product testing. Repeating these activities through notified bodies, when security outcomes can be equally achieved via internal procedures, introduces unnecessary cost and delays.²²

¹⁹ On average, it takes 33 months to develop a single harmonised standard, and the CRA standardisation request calls for more than 40 standards. Given the CRA's 36-month transition period, it is unrealistic to expect that the complete set of standards will be available on time. This challenge is compounded by the Commission's request to have standards ready by mid-2026.

²⁰ Art. 13 CRA, assuming the European standardisation organisations deliver the relevant horizontal standards by end October 2027.

²¹ Art. 32(2)(a) CRA. Full quality assurance (Module H) is also possible under Art. 32(2)(b).

²² As seen in the section above, this challenge is compounded by the fact that the CRA lacks the supporting infrastructure of harmonised standards needed for streamlined conformity assessment. Given the scope of the CRA and the number of products affected – especially in high-volume Class I categories – it is unlikely that sufficient harmonised standards or notified body capacity will be in place by the December 2027 deadline.



To remedy this, the digital package should **revert to design-type examination** for Module B, and **allow manufacturers to rely on self-assessment** for important products until a sufficient network of notified bodies is operational.

Limit reporting to the support period

The CRA allows manufacturers to define a support period for vulnerability handling and security updates.²³ However, under Art. 14, manufacturers remain obligated to report vulnerabilities and incidents without any reference to the declared support period. This creates a disproportionate burden for products that remain in use long after formal support has ended. It could force manufacturers to maintain reporting procedures – and legal exposure – for obsolete or unsupported products.

To remedy this, the digital package should **limit reporting obligations to the declared support period**. Once support has officially ended and this has been clearly communicated to users, no further reporting obligations should apply. This change would align reporting duties with a manufacturer's responsibility for maintaining the security of its products, and prevent unnecessary administrative burdens for legacy or out-of-support systems.

Allow RED-compliant products a CRA transition period

From August 2025, manufacturers will have to demonstrate compliance with the RED delegated act introducing binding cybersecurity requirements for radio equipment.²⁴ Beginning December 2027, the CRA will apply to an even broader range of digital products, many of which will overlap with those already subject to the RED.

Although the RED's and the CRA's security objectives converge, the way compliance must be demonstrated, including technical documentation and assessment procedures, is different. As a result, manufacturers will be required to undertake two separate conformity exercises for the same product, with redundant administrative and testing burdens, despite having satisfied equivalent cybersecurity legislation just two years earlier.

To address this, the digital package should introduce a **three-year transition period whereby products already placed on the market under the RED should be considered to have fulfilled the CRA's requirements**.²⁵


Tailor requirements for industrial systems

The CRA applies a uniform set of obligations across all product types, regardless of whether they are intended for consumer (B2C) or industrial/professional (B2B) use. This one-size-fits-all approach fails to reflect the operational realities of B2B environments, particularly in sectors involving complex systems, long

²³ Art. 13(8).

²⁴ Commission Delegated Regulation (EU) 2022/30, as amended by Commission Delegated Regulation (EU) 2023/2444.

²⁵ See Art. 6(a) CRA. Manufacturers should only need to demonstrate compliance with Annex I, Part II (on vulnerability handling), as required under Art. 6(b). This would avoid unnecessary duplication whilst still ensuring ongoing lifecycle requirements, such as patch management and disclosure policies, are upheld.



life cycles or specialised maintenance practices. The digital package should address this by introducing targeted clarifications to ensure proportionate and feasible compliance.

Clarify spare parts exemptions

Art. 2(6) CRA exempts spare parts under certain conditions, which may be too narrow for real-world maintenance practices in complex industrial installations. The digital package should:

- » Clarify that the spare parts exemption also covers functionally identical **full product replacements** used within complex systems – such as the substitution of a control unit or module in an industrial plant – where the replacement serves to maintain the system’s existing functionality and does not alter its design or operation.
- » Extend the exemption to **software-based support tools** used exclusively to commission, maintain or repair exempted spare parts or systems, where these tools do not add new functionality.

Accept compensating countermeasures

In industrial environments, strict adherence to the CRA’s cybersecurity requirements is not always technically feasible, especially when integrating new components into legacy systems or where full conformity would break interoperability.

To maintain both security and operational continuity, the digital package should formally recognise compensating security measures – as described in standards such as EN IEC 62443 – as valid alternatives in such cases. Manufacturers should be allowed to document these measures in installation or usage instructions, and reference them in the product’s technical file to demonstrate equivalent protection.

Exclude inherently low-risk products

The CRA’s horizontal scope encompasses inherently low-risk components such as toothbrushes, memory chips, analogue-to-digital (A/D) converters and basic sensors. These components, whilst digital, typically do not pose independent cybersecurity risks. Nevertheless, they are subject to the full suite of CRA obligations, including risk assessments, technical documentation and declarations of conformity.

The digital package could introduce an **explicit exclusion for ‘benign products,’** defined as components that can be shown to pose no meaningful cybersecurity risk when used as intended. This exclusion should be based on objective criteria, such as the absence of programmable logic, data connectivity or execution capability. A precedent exists in the Electromagnetic Compatibility Directive, which excludes passive and benign components on similar grounds.²⁶

²⁶ Recital 12, Directive 2014/30/EU.

FOR MORE INFORMATION, PLEASE CONTACT:

Rita Jonušaitė

Senior Manager for Cybersecurity & Cloud

rita.jonusaite@digitaleurope.org / +32 499 70 86 25

Sid Hollman

Policy Manager for Cybersecurity, Digital Infrastructure & Mobility

sid.hollman@digitaleurope.org / +32 491 37 28 73

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.