Position Paper on the Simplification of EU Cybersecurity Regulation

# Making EU cybersecurity regulation work for a dynamic European digital market

October 2025

The Computer & Communications Industry Association (CCIA Europe) welcomes the European Commission's efforts to simplify cybersecurity legislation in order to reduce costs for businesses and make the market more secure. In doing so, the Commission must go beyond streamlining reporting processes, and modernise the EU cybersecurity system as a whole. That is why CCIA Europe calls on the Commission to adopt a sweeping approach to simplification – delivering a truly competitive, secure, and open EU digital market.

## I. Optimising incident reporting

*Incident reporting should be proportionate, predictable, and consistent across the EU. A coherent reporting system will give regulators timely, comparable information; while allowing companies to focus on responding to incidents rather than duplicating paperwork.*

### Recommendations:

1. Unify templates, timelines, and thresholds across legislations
2. Allow a 'Report once, comply many' approach
3. Create a single, automated EU-level reporting platform
4. Standardise classification guidelines and key definitions

## II. Streamlining compliance management frameworks

*Clear, proportionate, and consistent compliance frameworks are essential. Simplifying obligations will reduce unnecessary administrative burdens, provide legal certainty, and allow companies to focus resources on improving innovative security solutions.*

### Recommendations:

5. Establish a unified EU compliance baseline
6. Provide clear EU-level guidance for consistent supervision
7. Standardise compliance reporting frameworks

## III. Harmonising certifications and ensuring workable supply chain security measures

*To strengthen the digital economy, certification and security measures must be consistent, practical, and interoperable. By consolidating schemes, recognising international standards, and supporting digital tools for compliance the EU can cut duplication, lower costs, and ensure that requirements genuinely enhance cybersecurity.*

### Recommendations:

8. Consolidate (fragmented) national certification schemes
9. Accept mutual recognition with international approaches
10. Allow automated evidence mapping

# Introduction

Over the past decade, the European Union has taken important steps to strengthen cybersecurity through legislation such as the Cybersecurity Act (CSA), NIS2 Directive, Cyber Resilience Act (CRA), Critical Entities Resilience Directive (CER), and the General Data Protection Regulation (GDPR).

These frameworks have helped raise Europe's collective resilience, but they have also created overlapping, and at times complicated obligations. Businesses operating across borders are confronted with fragmented reporting processes, inconsistent definitions, and duplicative requirements that consume resources without improving security.

Simplification is therefore essential. A coherent, predictable framework will allow companies to focus on strengthening security rather than navigating regulatory complexity. It will also give regulators access to higher-quality, comparable data and foster stronger cooperation between Member States, enabling a more effective EU-wide response to emerging threats.

The Computer & Communications Industry Association (CCIA Europe) believes the European Commission must seize this moment to deliver a truly competitive, secure, and open digital market. Our recommendations focus on three priorities:

I. Optimising incident reporting
   - Reduce fragmentation by harmonising templates, timelines, and definitions across legislations

II. Streamlining compliance management frameworks
   - Cut duplication by introducing a "Report once, comply many" approach and recognising cross-border audits

III. Harmonising certifications and ensuring workable supply chain security measures
   - Promote innovation and efficiency through automation, interoperability, and proportionate rules

By seriously approaching this opportunity to simplify, the EU can reduce costs, raise resilience, and strengthen trust in the digital economy.

# I. Optimising incident reporting

*Incident reporting should be proportionate, predictable, and consistent across the EU. A coherent reporting system will give regulators timely, comparable information; while allowing companies to focus on responding to incidents rather than duplicating paperwork.*

## 1. Unify templates, timelines, and thresholds across legislations

Currently, incident reporting obligations under NIS2, the Digital Operational Resilience Act (DORA), CRA, CER, GDPR and sectoral rules diverge significantly in terms of the templates, formats, and information required.[1] Companies must adapt their internal processes to multiple sets of requirements, which is both resource-intensive and confusing for staff. In practice, this means that for the same incident, a business may be forced to fill out several different forms, with inconsistent requirements on data points such as incident cause, impact, or remediation steps.

This fragmentation undermines the objective of EU harmonisation. By unifying templates, reporting deadlines, and severity thresholds, companies would spend less time navigating administrative complexity and more time responding to the incident itself. Importantly, harmonisation would also give regulators more consistent, comparable data across Member States, which is essential for building a coherent EU-wide situational awareness of threats.

## 2. Allow a 'Report once, comply many' approach

In sectors such as financial services, companies may face 20 to 40 different notifications for a single incident, covering EU agencies, national authorities, and sector regulators.[2] This duplication is a clear example of regulatory inefficiency: the same technical information is being reported repeatedly, without improving security outcomes.

A 'report once, comply many' mechanism would ensure that a single report is automatically distributed to all relevant authorities.[3] This approach is already used in other policy areas, and its adoption in cybersecurity would cut red tape significantly. It would also reduce the likelihood of inconsistencies across parallel reports and provide authorities with simultaneous access to the same information, improving trust and coordination.

## 3. Create a single, automated EU-level reporting platform

Even where incident reporting templates are aligned, companies are still forced to deal with multiple national portals and communication channels.[4] This imposes unnecessary costs on

[1] European Commission, *Impact Assessment for NIS2 Directive* (SWD(2020) 345); DLA Piper and Beltug, "Notification Requirements in the NIS2, DORA, GDPR: An Overview," DLA Piper, https://www.beltug.be/library/notification-requirements-in-the-nis2-dora-gdpr-an-overview/.
[2] European Cyber Security Organisation (ECSO), *Streamlining Regulatory Obligations: Action Plan*, July 2025, https://ecs-org.eu/activities/eu-legal-and-policy-task-force/.
[3] European Cyber Security Organisation (ECSO), *Streamlining Regulatory Obligations: Action Plan*, July 2025, https://ecs-org.eu/activities/eu-legal-and-policy-task-force/.
[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 22.12.2022, p. 80–152; Linklaters. "EU – NIS2: Three difficult implementation issues," Insights, June 12, 2025.

businesses that operate across borders, and it leaves regulators without a central overview. A single EU platform would streamline this process, serving as the central point for regulated entities while still allowing Member States access to the reports relevant to them. The European Union Agency for Cybersecurity (ENISA) could coordinate the technical aspects of this platform – such as data formats, security standards, and interface specifications – to ensure interoperability and trust across national systems.

Such a platform should be designed for interoperability. By supporting machine-readable formats and APIs, companies could integrate reporting directly into their security operations systems. This automation would reduce the scope for human error, speed up compliance during high-pressure incidents, and allow both authorities and businesses to focus their limited resources on incident response rather than administrative paperwork.

### 4. Standardise classification guidelines and key definitions

A key source of confusion in incident reporting is the lack of a uniform definition of what constitutes a reportable, major, or severe incident.[5] For example, under NIS2, reporting is triggered by different thresholds than under GDPR or DORA, leaving companies uncertain about when to notify.[6] This legal uncertainty encourages over-reporting in order to stay on the safe side, which provides regulators with minor notifications, making it harder to focus on serious threats.

Establishing clear, quantifiable definitions of reportable incidents such as thresholds based on duration, number of users affected, or economic loss would bring much-needed clarity. It would also reduce the administrative burden on entities and ensure that regulators only receive the most relevant, high-quality data. By standardising classifications across the EU, authorities could more easily compare incidents across sectors and Member States, strengthening Europe's collective cybersecurity posture.

## II. Streamlining compliance management obligations

*Clear, proportionate, and consistent compliance frameworks are essential. Simplifying obligations will reduce unnecessary administrative burdens, provide legal certainty, and allow companies to focus resources on improving innovative security solutions.*

[5] European Cyber Security Organisation (ECSO), *Streamlining Regulatory Obligations: Action Plan*, July 2025, https://ecs-org.eu/activities/eu-legal-and-policy-task-force/; Financial Stability Board, "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report." April 13, 2023; Baker McKenzie, *European Union: Who Does NIS2 Apply To and What Are the Key Obligations?*, February 2025.

[6] Rohma Fatima Qayyum and Syed Tatheer Kazmi, "EU Regulation 2025/302: ICT Incident Reporting for Financial Entities," Securiti. https://securiti.ai/eu-regulation-2025-302-overview/; Bernd Fiten and Wout Platteau, "24 hours, 72 hours, 1 month: the reporting of cyber incidents under NIS2," Timelex.https://www.timelex.eu/en/blog/24-hours-72-hours-1-month-reporting-cyber-incidents-under-nis2; Kristof Zadora and Dylan Verhulst, "Obligation to report incidents under the GDPR and the Belgian NIS2 Act," Monard Law. https://monardlaw.be/en/stories/informed/meldplicht-bij-incidenten-onder-de-gdpr-en-de-belgische-nis2-wet/#:~:text=Under%20the%20GDPR%2C%20organisations%20acting,freedoms%20of%20the%20data%20subjects.

## 5. Establish a unified EU compliance baseline

Today, companies must comply with a wide range of ongoing approval and certification obligations under NIS2, DORA, CSA, CRA, and national laws – from internal risk assessments to governance reporting and technical security measures. Although the objectives are similar, each Member State interprets and enforces these rules differently.[7] This leaves companies running duplicative audits and parallel compliance programmes, raising costs without improving security outcomes.

Establishing a harmonised baseline of approval and compliance obligations would allow businesses to maintain one robust security framework across the EU, rather than multiple slightly different ones. This also makes supervision more effective, giving regulators consistent evidence and freeing resources to focus on genuine risk reduction rather than procedural differences. This harmonised baseline should include a clear cross-walk or presumption-of-conformity mechanism, so that compliance with one recognised set of EU requirements can serve as evidence of compliance under others.

To make such harmonisation practical, EU and national authorities should also promote the use of interoperable, machine-readable formats and APIs to exchange compliance information automatically between systems and regulators. This would make supervision more effective, giving regulators consistent evidence and freeing resources to focus on genuine risk reduction rather than procedural differences.

## 6. Provide clear EU-level guidance for consistent supervision

Even where legislation is harmonised on paper, divergent supervisory practices and interpretations quickly reintroduce fragmentation (such as the interpretation of the legislative intent of 'main establishment' in the context of NIS2). This divergence highlights the need for EU-level guidelines to clarify legislative intent. National authorities and compliance bodies often interpret compliance obligations differently, leading to inconsistent expectations during audits and inspections.

Clear EU-level guidelines would ensure that compliance and approval obligations are applied consistently across Member States. This would reduce interpretative gaps, give companies certainty in building their compliance frameworks, and support supervisors in applying proportionate and predictable oversight.

## 7. Standardise compliance reporting formats

Currently, companies face a maze of different reporting templates and assessment formats when undergoing audits for cybersecurity compliance. Each supervisory authority may request the same information in slightly different ways, forcing companies to duplicate work. This lack of standardisation adds costs and makes it harder to compare results across markets.

Standardising compliance reporting formats across the EU would bring much-needed consistency. It would allow companies to prepare one comprehensive audit package that satisfies multiple authorities, freeing resources for substantive improvements rather than paperwork.

---

[7] European Commission, *Impact Assessment for NIS2 Directive* (SWD(2020) 345); European Cyber Security Organisation (ECSO), Streamlining Regulatory Obligations: Action Plan, July 2025, https://ecs-org.eu/activities/eu-legal-and-policy-task-force/;

# III. Harmonising certifications and ensuring workable supply chain security measures

*To strengthen the digital economy, certification and security measures must be consistent, practical, and interoperable. By consolidating schemes, recognising international standards, and supporting digital tools for compliance the EU can cut duplication, lower costs, and ensure that requirements genuinely enhance cybersecurity.*

## 8. Consolidate (fragmented) national certification schemes

Currently, Member States are developing their own certification schemes, and supply chain assessments also vary from one Member State to another.[8] For companies operating across borders, this creates an unmanageable tangle of obligations that are often duplicative or contradictory, but not necessarily better at identifying risks. Fragmentation also makes it harder for authorities to assess systemic risks consistently.

Consolidating these ICT certification schemes into single EU-level technical frameworks would bring clarity and predictability. It would also strengthen Europe's overall resilience by ensuring that risks are assessed according to common technical benchmarks, rather than diverging national approaches and political considerations that can leave gaps in collective defences.

Recent European standardisation work, such as CEN/TS 18026:2024 on cloud computing functional architecture and security requirements, already demonstrates the technical progress being made toward consistent, risk-based assurance frameworks across the EU. This work should continue to take the lead over Member State-specific standards and schemes. Importantly, such European schemes should remain voluntary, as currently envisaged under the CSA, a principle that should be preserved in its upcoming review.

Further, Member States, with the support of ENISA, the European Commission, and industry representatives should be encouraged to share and define common workable methodology to define non-technical criteria for supply chain in the context of the upcoming ICT Supply Chain Security Toolbox, rather than diluting the clarity and purpose of technical standards. This methodology should only complement existing regulation that includes supply chain security requirements including NIS2 and CRA, not making any additional measures to which would lead to potential duplication.

## 9. Accept mutual recognition with international approaches

European companies benefit from trade with suppliers and service providers from around the world which are already adopting rigorous security assessments (e.g. NIST CSF,

[8] Agence nationale de la sécurité des systèmes d'information (ANSSI), *SecNumCloud – référentiel de qualification des prestataires de services d'informatique en nuage*, version 3.2, March 2022, https://cyber.gouv.fr/secnumcloud; Bundesamt für Sicherheit in der Informationstechnik (BSI), *Cloud Computing Compliance Criteria Catalogue (C5)*, version 2020, https://www.bsi.bund.de/c5; European Cyber Security Organisation (ECSO), Streamlining Regulatory Obligations: Action Plan, July 2025, https://ecs-org.eu/activities/eu-legal-and-policy-task-force/; Théophane Hartmann, "Seventeen EU Countries Not Ready to Cut China 5G Dependence," Euractiv, March 18, 2025, accessed September 25, 2025, https://www.euractiv.com/news/seventeen-eu-countries-not-ready-to-cut-china-5g-dependence/.

ISO/IEC 27001).[9] Requiring companies to duplicate this evidence for EU purposes wastes resources without improving outcomes.

Mutual recognition of trusted international approaches would allow businesses to leverage existing certifications and attestations, while still ensuring that EU regulators receive the assurance they need. This would align Europe's cybersecurity framework with global practices, reduce compliance costs, allow EU companies to scale and grow into international markets, and make the EU a more attractive market for international operators.

This is all the more relevant as upcoming standards for the Cyber Resilience Act (CRA) are being developed to guide essential security requirements' interpretation and implementations for products with digital elements. Recognising existing international frameworks is critical to prevent new hardware and software products from being stalled by a backlog of conformity assessment body reviews, especially where clear international benchmarks already exist, as companies take the necessary time to ensure their products and services are up to the international standards requirements. This proactive recognition would ensure a smoother transition and maintain market flow.

### 10. Allow automated evidence mapping

Much of compliance today involves manually transferring data from one system into another, a process prone to error and costly in staff time. By promoting automated evidence mapping (e.g. leveraging machine-readable formats like OSCAL) in compliance frameworks and processes, companies could re-use security evidence across multiple frameworks and share it digitally with regulators.

Supporting digital solutions such as standardised machine-readable formats, APIs, and interoperability between compliance platforms would reduce administrative overhead, scale compliance processes to keep the pace of innovation, and make it easier for both businesses and regulators to track and verify supply chain security. Automation would also support effective and efficient exchange of information between entities and supervisors, allowing entities to focus on actionable outcomes rather than paper-based processes. Automation also allows faster responses when new risks emerge, ensuring Europe's supply chains remain resilient.

[9] Zach Meyers, *"Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?"* (Issue Paper, Centre on Regulation in Europe, September 2025), https://cerre.eu/wp-content/uploads/2025/09/CERRE_Issue-Paper_EU-Competitiveness_Can-the-EU-reconcile-digital-sovereignty-and-economic-competitiveness.pdf; Heather Buker, "NIST Cybersecurity Framework: Frequently Asked Questions Answered!," *6clicks* (blog), December 7, 2022, accessed September 24, 2025, https://www.6clicks.com/resources/blog/nist-csf-frequently-asked-questions-answered; "Apple Legal — Privacy: Governance," *Apple,* accessed September 24, 2025, https://www.apple.com/legal/privacy/en-ww/governance/; "What Is ISO/IEC 27001?," *IBM*, accessed September 24, 2025, https://www.ibm.com/products/cloud/compliance/iso-27001.

## Conclusion

In simplifying the EU's cybersecurity legislative framework, the European Commission should adopt a holistic approach that extends beyond reporting processes. It should cover incident reporting, compliance frameworks, certification obligations, and supply chain security, where necessary and proportionate.

The scope of legislative proposals must remain firmly technical, ensuring that requirements address genuine cybersecurity concerns, while non-technical aspects are dealt with through other instruments. By seriously approaching this opportunity to simplify, the EU can reduce costs, raise resilience, and strengthen trust in the digital economy.

## About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

**For more information, please contact:**
CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org