DIGITALEUROPE

20 JUNE 2025

Updating the EU cybersecurity framework: Industry priorities for the Cybersecurity Act revision

Executive summary

The EU's cybersecurity framework has undergone substantial expansion since the adoption of the Cybersecurity Act (CSA) in 2019.[1] Alongside the CSA, new legislative instruments – including NIS2, the Cyber Resilience Act (CRA), DORA and the Cyber Solidarity Act – now define a much more comprehensive and multi-layered regulatory architecture for cybersecurity across the single market.[2]

In this context, the CSA review presents an opportunity to strengthen the role of certification as a practical tool for legal interoperability, regulatory coherence and market trust. At the same time, experience with the implementation of the CSA has highlighted areas where targeted improvements are needed to ensure that certification schemes are effective, market-relevant and fully aligned with both technological realities and business models.

The review must preserve the CSA's original balance: enabling cybersecurity resilience whilst safeguarding competitiveness and innovation. Certification should serve as a facilitative instrument that supports businesses, avoids unnecessary regulatory layering and integrates coherently with existing and emerging EU legislation. In parallel, the CSA review should clarify ENISA's mandate and strengthen its role in supporting technical consistency, certification development, vulnerability management and international cooperation, whilst respecting the distinct mandates of other EU bodies.

This paper aims to contribute constructively to the CSA review process, drawing on the experience of both ICT providers and users across sectors. Our proposals seek to ensure that the CSA remains a cornerstone of European cybersecurity policy, delivering effective, proportionate and globally interoperable outcomes.[3]

---

[1] Regulation (EU) 2019/881.

[2] Directive (EU) 2022/2555 and Regulations (EU) 2024/2847, 2022/2554 and 2025/38, respectively.

[3] This paper expands upon DIGITALEUROPE's earlier contribution to the CSA evaluation, *Adapting ENISA's mandate and collaboration in a changing cyber landscape*, available at https://cdn.digitaleurope.org/uploads/2023/09/DIGITALEUROPE_Adapting-ENISAs-mandate-and-collaboration-in-a-changing-cyber-landscape.pdf.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

Our key recommendations are to:

- **Preserve the voluntary nature of certification as the general rule**. Mandatory certification should remain limited to well-defined high-risk use cases, with any expansion subject to full assessment of proportionality and market impact.
- **Strengthen certification as a legal interoperability tool across the EU cybersecurity rulebook**. Certification schemes should serve as recognised instruments to demonstrate compliance with technical obligations under other frameworks, minimising duplicative assessments.
- **Accelerate the development of certification schemes**, with clearer governance, transparent processes and predictable adoption timelines.
- **Improve governance and stakeholder involvement**, including a stronger role for stakeholders, transparent interaction with Member States and clearer separation between the technical preparation and adoption phases.
- **Ensure full harmonisation of certification baselines across Member States**, with narrowly defined national deviations only where strictly necessary to address unique security concerns.
- **Align EU certification schemes with international standards** to maintain global interoperability, reduce compliance costs and support European industry's global competitiveness.
- **Expand ENISA's mandate**, enabling the Agency to concentrate on certification development, policy advisory functions, regulatory coherence, international cooperation and vulnerability management, whilst avoiding institutional overlaps with other EU bodies.
- **Support ENISA's role in vulnerability disclosure** by enhancing its contribution to the global CVE system and ensuring alignment between European and international vulnerability identifier systems.
- **Maintain the European Cybersecurity Competence Centre's (ECCC) lead role on cybersecurity skills development**, with ENISA providing strategic input.

DIGITALEUROPE remains committed to working with the EU institutions and Member States to ensure effective, coherent and globally competitive cybersecurity outcomes for Europe.

Table of contents

The CSA's role within the EU cybersecurity framework

The CSA serves as both the Union's horizontal framework for cybersecurity certification and the legal basis for ENISA's permanent mandate, establishing its role in supporting EU policy coordination, operational cooperation and the development of European cyber capabilities.

Certification remains central to the CSA's practical contribution to European cyber resilience. By developing harmonised certification standards for ICT products, processes and services, coordinated by ENISA, the CSA supports the single market and strengthens Europe's digital competitiveness.

Avoiding premature new obligations

The EU's cybersecurity regulatory landscape has been expanding rapidly, with the adoption of multiple frameworks. In addition to an enhanced NIS2, which establishes comprehensive cybersecurity risk management and reporting obligations for a wide range of entities across critical sectors, the CRA introduces extensive supply chain security obligations across hardware and software products. These requirements remain in the early stages of implementation, and their full practical impact has yet to be assessed.

In this context, the introduction of any additional obligations would be most unhelpful. The CSA review should not introduce any new certification obligations before the effects of existing legislation are fully evaluated. Instead, efforts should focus on strengthening the interoperability and complementarity of certification schemes as an instrument to support compliance across the broader EU rulebook.

Enhancing supply chain security through guidance

Rather than expanding obligations, the CSA should promote the development of structured guidance on comprehensive supply chain risk assessments, building on international standards such as ISO 27001, ISO 31000 and the NIST Cybersecurity Framework. This would enable organisations to avoid duplicate compliance frameworks to identify, prioritise and manage supply chain risks, including through collaboration with suppliers and subcontractors. Standardised approaches to supply chain risk management would support critical sectors in maintaining resilient supply chains aligned with global best practices.

Preserving the CSA's fundamental security objectives

The CSA's original security objectives remain valid and should not be revisited or redefined. Rather, the focus of the review should be on targeted improvements to streamline implementation, ensure legal interoperability with other EU legislation and close identified gaps in the certification development process.

Certification should be strengthened as a practical enabler of resilience and market trust, supporting competitiveness without becoming a blanket compliance instrument.

Positioning certification within the broader EU legal framework

The CSA must operate as an integrating legal instrument across the EU's regulatory architecture. Without a coherent approach to legal interoperability, overlapping security obligations under different instruments will continue to impose duplicative requirements on businesses, particularly where certification may be called upon to demonstrate compliance with multiple legislative acts.

In this respect, the CSA should serve as a central reference framework for demonstrating compliance with technical security requirements under other EU instruments, including:

- NIS2: certification schemes should serve as recognised mechanisms to demonstrate compliance with technical and organisational measures for Essential and Important Entities.
- CRA: certification schemes should serve as a voluntary pathway for demonstrating compliance with the CRA. Where an EU cybersecurity certification scheme exists, products certified under the CSA should be presumed to meet the corresponding CRA obligations, without the need for additional delegated acts to re-assess their adequacy.
- Cyber Solidarity Act: Certification schemes should support the operationalisation of the EU Cybersecurity Reserve, providing a basis for security assurance of managed security service providers.
- General Data Protection Regulation (GDPR):[4] Certification schemes adopted under the CSA should be recognised to demonstrate compliance with relevant GDPR security obligations.[5] By the same token, GDPR certifications should be considered as evidence of compliance with relevant cybersecurity requirements. Mutual recognition of certifications across both frameworks should be promoted to reduce duplicative assessments and enhance legal coherence.
- Sector-specific legislation: European cybersecurity certification schemes should be developed in a way that allows ICT service providers to use them as a recognised means of demonstrating compliance with relevant sectoral security obligations, including for regulated sectors such as financial services, energy and health.[6] To avoid fragmentation, sector-specific needs should be addressed through risk assessments and supervisory guidance layered onto horizontal certification schemes, rather than through the creation of sector-specific certification frameworks.
- Incident reporting: Certification should interface with the development of a single EU incident notification platform, to streamline reporting obligations across multiple legislative instruments.[7]

Certification framework

Limited practical implementation to date

At present, only one European cybersecurity certification scheme – the Common Criteria-based Cybersecurity Certification Scheme (EUCC) – has been adopted under the CSA and remains limited in both scope and applicability.[8] As a result, most economic operators active in the single market have limited or no practical access to EU cybersecurity certification pathways. The Union Rolling Work Programme (URWP) has not yielded the expected pipeline of additional schemes, and the system remains largely

[4] Regulation (EU) 2016/679.

[5] Art. 32 GDPR.

[6] This is particularly relevant under DORA, where financial entities are responsible for oversight of their ICT third-party providers.

[7] This matter is addressed in more detail in our position on the simplification of cybersecurity rules, available at https://cdn.digitaleurope.org/uploads/2025/06/Digital-simplification-package-Cyber.pdf.

[8] Commission Implementing Regulation (EU) 2024/482.

theoretical.[9] The gap between legal ambition and operational delivery increasingly undermines the relevance of the framework.

Further progress is necessary both to accelerate the development of market-relevant schemes and to clarify the interplay between EUCC and other frameworks. In particular, the CSA review should provide greater legal certainty regarding the extent to which EUCC certification may be used to demonstrate conformity under the CRA, including for products incorporating open-source components. Similarly, mutual recognition of Common Criteria certifications under the EUCC should be pursued to maximise efficiency and avoid duplicative assessments.

Voluntary certification as the general rule

The voluntary nature of certification under the CSA must remain a core principle. Whilst wider adoption of cybersecurity certification schemes is desirable, universal or horizontal mandatory certification is neither practical nor proportionate at this stage.

Certification must be deployed in a manner that supports digital resilience without introducing disproportionate burdens, distorting time-to-market dynamics or inhibiting software development cycles.

The CSA already requires that any decision to make certification mandatory must follow a detailed assessment of existing schemes and their appropriateness.[10] This balance, carefully negotiated during the adoption of the CSA, should be fully preserved.

Where mandatory certification is deemed necessary, this should be limited to high-risk applications identified in sector-specific legislation based on clear and predictable criteria, as exemplified by the approach taken in the CRA for 'critical products.' In parallel, non-binding guidance should be developed to assist Member States and procurers in using certification schemes appropriately within national practices.

The CSA should also explicitly recognise certification as a means of demonstrating compliance with technical obligations under related EU legislation, to incentivise voluntary uptake and promote legal interoperability across regulatory regimes.

Stakeholder involvement and governance

Effective certification depends on structured stakeholder participation, transparency and predictability in scheme development. This is essential to ensure that schemes are technically sound, proportionate and reflective of actual needs and implementation realities.

Whilst the CSA established both the European Cybersecurity Certification Group (ECCG) composed of Member States and the Stakeholder Cybersecurity Certification Group (SCCG), the governance structure has remained unbalanced. The SCCG must be systematically involved from the inception of scheme development, empowered to issue non-binding opinions, and granted effective visibility over drafting processes and timelines.

[9] SWD(2024) 38 final.

[10] Art. 56(3) CSA.

Structured interaction between the SCCG and ECCG should be institutionalised through joint meetings and systematic information exchange. Impact assessments of proposed schemes should systematically incorporate SCCG input, leveraging the group's breadth of technical and market expertise.

The URWP must be strengthened as a credible forward-planning tool, providing full transparency on upcoming certification initiatives and ensuring that stakeholders have sufficient time and visibility to mobilise their expertise.

To reinforce the integrity of the process, the schemes' technical preparation should remain clearly distinct from their formal adoption. The Commission should continue to exercise its responsibilities for adopting implementing acts but should refrain from making substantive technical modifications once scheme drafts have been finalised. The ECCG chairmanship should rotate along the Council Presidency model, and ENISA should assume full chairmanship of the SCCG, reflecting its secretariat role.

Finally, ENISA should be empowered to establish standing and ad-hoc expert groups to address identified technical gaps to ensure that schemes remain technologically current and operationally viable.[11]

Self-assessment as standard

Vendor self-assessment should be the default conformity assessment pathway for most products and services. Third-party evaluation should be reserved for higher assurance levels or high-risk applications where objective risk analysis justifies additional oversight.

Well-documented self-assessments, supported by standardised evidentiary materials, can provide sufficient assurance whilst minimising unnecessary costs. Third-party conformity assessment bodies can support the self-assessment process by developing standardised tools and templates to ensure consistency. This approach is particularly important to maintain accessibility for SMEs, startups and open-source contributors, and to preserve the competitiveness of European digital industries.

Harmonised EU security baselines

Certification baselines must be fully harmonised across the Union. Divergent national requirements undermine the internal market and erode confidence in the certification framework.

Common EU baselines should reflect shared risk scenarios applicable across all Member States. Where exceptional national security considerations exist, deviations should be strictly limited to narrowly defined supplementary controls building on the highest common assurance level. This would allow Member States to address specific concerns without undermining pan-European consistency.

Certification schemes should remain technology neutral, and outcome focused, avoiding over-prescriptive, sector-specific or use-case driven customisations that risk proliferating fragmented schemes and diluting available expertise.

[11] Including notably for open-source software security.

Alignment with international standards

Alignment with established international standards remains essential to the competitiveness and global interoperability of European certification schemes.

The EU should build upon existing standards developed by international bodies such as ISO, IEC and NIST. Developing entirely new European standards in isolation would be too resource-intensive and slow and would reduce market access for European technologies in third countries. Leveraging globally accepted frameworks allows faster deployment and supports European companies operating globally.

International mutual recognition of certifications, where technically feasible and politically acceptable, should be actively pursued, including through recognition of equivalent evaluations performed by accredited conformity assessment bodies in third countries. Mutual recognition frameworks can also serve as platforms for broader international cooperation, fostering shared learning and convergence across jurisdictions.

Any EU-specific deviations should be limited and fully justified.

Phasing out national schemes

Clear and enforceable rules are required to govern the transition from national certification schemes to EU-level schemes.

The CSA should specify binding sunset clauses for national schemes once equivalent EU schemes are operational. During transition periods, mutual recognition mechanisms should be established to preserve market access and avoid disruption. Grandfathering provisions should allow existing national certifications to be recognised or migrated into corresponding EU schemes.

The absence of clear transition arrangements risks prolonging fragmentation and undermining the value proposition of EU-level certification.

ENISA's role

Strategic focus and mandate recalibration

ENISA's expanding role within the EU cybersecurity framework is necessary and welcome, but must be supported by a clearer mandate, sharper priorities and adequate resources. Despite growth since the CSA's adoption, ENISA remains under-resourced relative to the scale of its assigned missions, particularly against the backdrop of heightened geopolitical tensions and systemic cyber threats.

To ensure long-term relevance and operational effectiveness, ENISA's mandate should be recalibrated to focus on areas where it can deliver distinct European added value, whilst avoiding institutional overlaps with other EU bodies. ENISA should prioritise:

- Strengthening a common EU cybersecurity baseline by promoting regulatory consistency and supporting harmonised implementation of EU law;
- Reducing internal market fragmentation, including through leadership in cybersecurity certification development; and

- Advising on the cybersecurity dimensions of new EU legislative proposals, providing early-stage policy input.

ENISA's operational focus should centre on implementation, coordination and policy support rather than replicating policy design or supervision roles entrusted to sectoral authorities or EU supervisory bodies.

Clarifying responsibilities vis-à-vis other EU bodies

The growing number of EU entities with partial cybersecurity mandates has led to institutional fragmentation. In several instances, competences originally assigned to ENISA have been allocated to parallel structures without a coherent division of labour. This risks undermining the original objective of developing ENISA into the Union's centre of cybersecurity expertise.[12]

A conceptual framework is required to delimit ENISA's remit vis-à-vis entities such as the ECCC, sectoral authorities – including the three European supervisory authorities for finance, the European Data Protection Board (EDPB), the AI Office – and the European Commission itself. This will allow ENISA to serve as the principal coordination platform for technical policy interpretation, cross-sectoral information sharing and regulatory consistency.

Strengthening ENISA's policy advisory function

ENISA should be systematically involved in the preparatory stages of EU legislative and regulatory initiatives that involve cybersecurity dimensions. As part of this role, the Commission should systematically seek ENISA's expert input on the cybersecurity implications of new sectoral legislation, including through formalised mandatory cybersecurity assessments during the legislative drafting process.

In parallel, ENISA should be empowered to issue guidance on the interpretation of cybersecurity obligations under EU law, to support consistent implementation across Member States and promote convergence of supervisory practice. To ensure effectiveness, mechanisms should be developed to give ENISA guidance greater normative weight within Member States' implementation processes, whilst remaining within ENISA's technical advisory mandate.

Certification leadership

Certification development should be strengthened as a core responsibility of ENISA. In particular, ENISA should:

- Lead the technical preparation of candidate certification schemes, including drafting technical specifications and managing expert consultations;
- Provide guidance on scheme implementation and oversee testing phases; and
- Coordinate with the SCCG (as Chair) and the ECCG (through structured subgroup arrangements) to ensure inclusive stakeholder participation.

This role would enable ENISA to deliver technically robust, market-relevant schemes whilst ensuring effective stakeholder input, predictable development timelines and alignment with EU policy priorities.

[12] Art. 4(1) CSA.

Enhancing public-private collaboration

Public-private cooperation remains critical to strengthening European cyber resilience. In addition to the SCCG and existing advisory structures, ENISA should facilitate the creation of a Joint Public-Private Cybersecurity Expert Group, composed of CISOs and industry leaders, to advise on strategic threat mitigation, sectoral implementation challenges and emerging policy risks.

This strategic unit would serve to ensure that ENISA's workstreams remain grounded in operational realities and that industry expertise is systematically incorporated into the Agency's deliverables.

International cooperation

ENISA should strengthen its international engagement, leveraging its institutional independence to serve as the Union's interlocutor with key third-country cybersecurity agencies, including the US Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC), with a view to fostering cross-border convergence.

International cooperation should also extend to technical collaboration on certification, standardisation, vulnerability management and threat intelligence sharing. This external dimension is increasingly critical to ensuring the global relevance of European cybersecurity governance.

Vulnerability management and alignment with CVE system

ENISA's role in vulnerability disclosure should be expanded and aligned with global vulnerability ecosystems.

The Common Vulnerabilities and Exposures (CVE) system is the globally recognised framework for identifying and cataloguing publicly disclosed cybersecurity vulnerabilities. ENISA's designation as a CVE Numbering Authority (CNA) and its stated ambition to assume the role of Root CNA for Europe are positive developments that should be supported with dedicated resources and infrastructure, including mirrored infrastructure in Europe co-developed with international partners. EU institutions should actively support this objective in transatlantic and multilateral cybersecurity dialogues.

At the same time, improved coordination between the ENISA-operated European Union Vulnerability Database and the global CVE system is necessary to avoid divergent identifier systems that risk confusing market participants and undermining software supply chain security. Incompatibility between vulnerability identifiers poses significant risks for software bill of materials (SBOM) adoption and vulnerability disclosure processes, leading to conflicting data sets for industry and operators of essential services.

We encourage the Commission to fully support ENISA's leadership role in driving global alignment on vulnerability taxonomy, identifier systems and technical standards for vulnerability management.

Finally, we reiterate that public vulnerability reporting should occur only after adequate mitigation or corrective actions have been implemented, to avoid increasing exposure for defenders and critical infrastructure operators.[13]

[13] This is addressed in more detail in our position on the simplification of cybersecurity rules, pp. 6–7.

Skills and workforce development

The ECCC should assume primary responsibility for the coordination of cybersecurity skills development programmes and funding initiatives. ENISA should provide strategic input, leveraging its technical expertise, but should not assume an operational role in skills development, which risks duplicating the ECCC's mandate.

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.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20