bitkom

Position Paper

June 2025

Cybersecurity Act Revision

Summary

The Cybersecurity Act (CSA) was introduced in 2019 as a central instrument of the European Union to strengthen the cyber security of information and communication technologies. At the time, there were no other European harmonized requirements for products concerning cybersecurity. The focus of the CSA was strengthening the mandate of the EU agency ENISA and creating the European Cybersecurity Certification Framework (ECCF) for the voluntary certification of ICT products, services and processes. In the meantime, however, the regulatory landscape has evolved significantly: With the Network and Information Security Directive 2 (NIS2), the Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA) and the delegated Radio Equipment Directive (RED), a large number of other regulations have come into force with partially overlapping requirements or are about to be implemented. Instead of providing clarity and harmonisation, the CSA is itself becoming part of an increasingly fragmented system. Companies are confronted with parallel reporting obligations, different national implementation practices and regulatory duplication. This threatens to reverse the goal of a resilient digital infrastructure: Security is not created through complexity, but through impact.

It is precisely in this situation that the CSA has an important role to play - not only as a certification framework, but also as a coordinating element for coherence and simplification. Bitkom is therefore clearly in favour of a targeted revision of the CSA Regulation. This includes, in particular, strengthening ENISA as the central authority for technical implementation aids for NIS2. Equally important is a paradigm shift in the certification process: The procedures must be made more transparent and accessible, stakeholders must be more broadly involved, and certification schemes must be strictly limited to technical criteria. Current practice – as in the case of the EUCS scheme - clearly shows the weaknesses of the existing model: a lack of transparency, a lack of official drafts and the influence of geopolitical considerations are blocking progress. However, a functioning European single market for cybersecurity needs fast, comprehensible and industry-supported certifications – for example in the area of 5G, where EU-wide recognition is urgently needed.

Under these circumstances, the CSA revision must also address the increasing complexity arising from overlapping legislative requirements – most notably between the NIS2 Directive and the CRA. Bitkom therefore welcomes the Commission's intention to use the CSA review as a vehicle for regulatory simplification. The current patchwork of obligations, especially regarding cybersecurity incident reporting, creates unnecessary burdens for companies and authorities alike. As it stands, both NIS2 and CRA introduce nearly identical reporting timelines but through separate mechanisms and actors—potentially resulting in up to six parallel reports for a single incident. EU regulation should be guided by the principle of «one incident, one report, one reporting mechanism«. Achieving this will require a clearer delineation of reporting responsibilities, consistent definitions across legal acts, and adjustments to ENISA's mandate.

ENISA Mandate

Bitkom advocates for a targeted strengthening of ENISA. Both the NIS2 Directive and the CRA assign ENISA a substantial number of new responsibilities, which require consistent implementation and coordination at the European level. Under the NIS2 Directive, these tasks include the development and maintenance of registries for vulnerabilities and cross-border services, the coordination of best practice sharing among Member States and within the European Cyber Crises Liaison Organization Network (CyCLONe), as well as the annual reporting on the state of cybersecurity across the EU. From our perspective, this annual report should specifically cover the progress made in the dissemination of cybersecurity best practices at the European level, initiatives for regulatory simplification, cooperation between designated national authorities, harmonisation efforts and remaining gaps, and include concrete suggestions for improvement.

Within the CRA, ENISA is likewise assigned several key responsibilities. These include the development and maintenance of the single reporting platform for vulnerabilities, support for the implementation of the regulation, the development of new EU cybersecurity certification schemes, the provision of technical reporting on product-related cybersecurity trends in Europe, and, upon request, further support across various aspects of CRA implementation.

In addition to its operational and coordination tasks under NIS2 and the CRA, ENISA should take on an important role in promoting regulatory coherence and supporting implementation through practical tools. To this end, Bitkom recommends that ENISA conduct a comprehensive analysis and mapping exercise to identify areas of regulatory fragmentation across the EU. This exercise should be based on internationally recognised standards and aim to propose concrete measures for simplification and harmonisation. To further support compliance efforts by both national authorities and regulated entities, ENISA should map existing standards against the security requirements of relevant EU regulations. This mapping should adopt a risk-based approach, highlight any gaps in coverage, and recommend additional measures where needed. Particular emphasis should be placed on clarifying the interplay between EU regulatory requirements and international standards. Established frameworks, such as

ISO/IEC 27001, should serve as the foundation for demonstrating compliance wherever possible.

ENISA should be empowered to drive forward the development of a harmonised, cross-sectoral reporting framework for security incidents under the CSA. Currently, reporting obligations are fragmented across multiple regulatory instruments—namely NIS2, DORA, CRA and the GDPR—each with its own set of thresholds, deadlines and reporting channels. A centralised reporting portal, underpinned by harmonised standards, would substantially enhance legal clarity and strengthen the ability of competent authorities to detect and respond to cyber threats. At the same time, it is essential to prevent redundant reporting obligations and the risk of multiple sanctions in the case of cross-border incidents. ENISA should take on a coordinating role in this area, including the development of interoperable systems, aligned threshold definitions and standardised reporting procedures.

Moreover, ENISA should be tasked with developing best-practice guidelines that consolidate Member States' approaches to incident handling and apply the once-only principle – ensuring incident information is reported once and reused securely across authorities.

An additional aspect that is currently not sufficiently reflected in ENISA's mandate is the structured evolution of European cybersecurity certification schemes, such as EUCC. This is a critical task to ensure that certification frameworks remain effective and up to date in light of the rapidly evolving cybersecurity threat landscape. To guarantee that certification schemes are regularly reviewed and updated, the CSA must establish the necessary institutional and procedural structures.

The active and continuous involvement of industry stakeholders is also essential for the sustainable and practical evolution of cybersecurity certification schemes. Bitkom recommends the establishment of structured Public-Private Partnership models to leverage industry know-how in alignment with the EU's strategic cybersecurity objectives. Such a collaborative approach would ensure that certification remains relevant, implementable and technically robust. Accordingly, the upcoming revision of the CSA should include an explicit expansion of ENISA's mandate to cover scheme maintenance and ensure that the agency is equipped with the financial and human resources required to fulfil this role effectively.

European Cybersecurity Certification Framework

Cybersecurity certification schemes under the ECCF have the potential to play a central role in ensuring regulatory compliance within an increasingly complex and evolving regulatory landscape. Schemes such as the European Union Cybersecurity Certification Scheme (EUCC) can be instrumental in demonstrating conformity with requirements under key regulatory frameworks, including the NIS2 Directive, the DORA, and the CRA. In this context, certification can offer legal certainty and reduce the burden of proof for companies seeking compliance with these horizontal and sector-specific regulations. In addition, industry-led schemes such as the Network Equipment Security Assurance Scheme (NESAS) by the Global System for Mobile Communications Association can play

a vital role by complementing European efforts with sector-specific expertise and fostering international alignment.

The growing interdependence of European cybersecurity legislation and certification efforts underscores the importance of establishing a coherent and harmonised approach to certification. EU-wide schemes like the EUCC have the capacity to harmonise requirements across Member States, thereby reducing administrative and compliance costs – especially for operators that are active in multiple countries. Inconsistent national certification schemes and diverging interpretations of regulatory obligations currently contribute to market fragmentation. European schemes offer a path to simplification and legal clarity.

To fully realise their potential, however, EU cybersecurity certification schemes must be firmly aligned with international standards. Global acceptance of certification outcomes depends on the relevance and interoperability of European schemes in markets beyond the EU. Ensuring international compatibility will not only support European companies in global competition but also prevent the emergence of isolated or overly EU-specific requirements that could create barriers to market entry.

Despite their significant relevance, the current pace of development and adoption of certification schemes under the ECCF remains too slow. To address this, Bitkom proposes the introduction of a structured and inclusive consultation process. When the European Commission issues a request to draft or update a certification scheme, ENISA should be first tasked with conducting a coherence study to assess the alignment with existing schemes and relevant legislation. Following this, a feasibility analysis should be carried out based on input from industrial stakeholders and so-called "risk owners." This would ensure that certification schemes are realistic, targeted, and delivered more efficiently. Moreover, formal opportunities for stakeholder input should be embedded throughout the drafting process, particularly when significant changes to the initial draft are considered. Including the expertise of leading cybersecurity providers will improve the quality of the schemes and support their adoption in the market.

The relevance of certification under the ECCF has been significantly amplified by the introduction of product legislation such as the CRA and its integration into the New Legislative Framework. Certification schemes like EUCC are envisaged not only to demonstrate technical security compliance but also to facilitate smooth market access. To fully realise this dual role, the European Commission should establish in relevant product legislation – such as the CRA or the AI Act – that certification under a corresponding scheme pursuant to the CSA gives rise to a presumption of conformity. This would ensure legal certainty and consistency across legislative instruments, avoiding fragmented or overlapping certification requirements. While this objective cannot be achieved through the revision of the CSA, the Commission should aim to implement these changes in the upcoming omnibus package on simplification.

Finally, it is essential that the CSA review ensures alignment between certification schemes and ongoing standardisation efforts. The duplication of existing workstreams must be avoided to ensure regulatory coherence and efficient use of industry resources. Certification should complement, not conflict with, standardisation initiatives already underway in recognised bodies.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Felix Kuhlenkamp | Head of Cybersecurity
P +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Responsible Bitkom committee
WG Security Policy