Standardisation for the Cybersecurity Act 2

DIN position for the consultation on the Cybersecurity Act 2

MAY 2026

- It is important to closely align the CSA2 and the existing standardisation system to reinforce Europe's role in international standardisation and avoid additional barriers to market entry.
- The European Standardisation Organisations (ESO) CEN and CENELEC are currently working on improvements to the European Standardisation System (ESS). This improved ESS should function as the preferred framework for generating, integrating, managing, and using technical content. This would speed up standards-delivery for ENISA and ensure that the EU continues to harness the efficiencies of international standardisation for the European economy.
- Rework Article 100(4)(a) to avoid a blanket statutory prohibition on participation in European cybersecurity standardisation. Instead, the Commission should rely on the established mechanisms of the transparent, inclusive and consensus-oriented ESS to successfully mitigate non-technical risks.
- Anchor the CSA2 rules for conformity assessment in horizontal European legislation and rely on ISO and/or IEC conformity assessment standards (notably EN ISO/IEC 17065) to avoid unnecessary costs.

Christoph Tovar
Senior Manager Government Relations
Tel.: +49 (0) 30 2601-2144
E-Mail: christoph.tovar@din.de

Martin Uhlherr
Team Coordinator
Tel.: +49 (0) 30 2601-2591
E-Mail: martin.uhlherr@din.de

Utilizing European Standardisation

The proposed Cybersecurity Act 2 (CSA2) seeks to strengthen Europe's cyber resilience. Amongst various changes, it aims to better align standards development with ENISA's needs and better handle non-technical risks.

DIN is the national standardisation body of Germany. As such we would like to recommend certain changes to the CSA2 draft, that allow it to achieve its aims while avoiding certain negative implications. Particularly, we recommend three things: Firstly, to **advance the process of European standards development instead of creating a parallel standard setting system**. Secondly, to **build on the inclusiveness of European standardisation** to mitigate non-technical risks. And thirdly, to **avoid unnecessary cost and bureaucracy by duplicating standards** for conformity assessment.

BENEFITING FROM THE EUROPEAN STANDARDISATION SYSTEM

Article 18(1) provides that ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity, and Article 18(2) adds that ENISA shall "monitor and, where relevant, participate and lead in standardisation development activities". Various segments of the CSA2 draft, like recital 40 or Article 77 (3), specify that ENISA should develop technical specifications, where a need for any technical detail specification has been perceived and relevant standards do not yet exist. **Technical specifications developed by ENISA therefore appear to be the new preferred instrument for specifying necessary technical details**.

DIN supports ENISA's role as a centre of expertise and a provider of technical advice to the Commission and Member States. However, requiring ENISA to preferably draft technical specifications and to "lead" standardisation development **will create a de facto parallel standard-setting track outside established, open, and consensus-based processes**. Two negative consequences would arise from this approach: Firstly, European experts would be required to reallocate their already scarce resources to develop technical specifications for ENISA. This would weaken the ability of European businesses to set global cybersecurity standards within international standardisation organisations. Ultimately, this would be weakening the competitiveness of European businesses on international markets. Secondly, creating an ENISA-centered system of technical specifications poses the risk of divergent European and international standards, thus creating unnecessary market barriers and economic inefficiencies.

DIN understands the **need for faster development** of European Cyber Certification Schemes and **relevant standards. Similar issues are currently discussed as part of the ongoing revision of the European standardisation regulation** (1025/2012).[1] We expect a proposal for the new standardisation regulation in September 2026. Furthermore, the European Standardisation Organisations CEN and CENELEC are internally working on further improving processes for standardisation delivery. Crucially, this will also include a process for adopting technical content from Common Specifications, consortia, open-source communities, and other standards developing organisations into the European standardisation process entrusted to CEN and CENELEC. In combination with general improvements to the standardisation process, this would enable faster and more open development of standards, while maintaining necessary coherence across the European standards landscape and support Europe's role in global standardisation. DIN believes that the currently initiated reforms for the ESS are sufficient to meet ENISA's need for better standards development. **We therefore recommend, that CSA2 utilizes**

[1] C.f. DIN 2025.

the improved European Standardisation System instead of creating an additional standard-setting track within ENISA.

DIN recommends:

- Clarify, that the **development of technical specifications** foreseen in Article 18(1) only **functions as an instrument of last resort**. The European Standardisation System should continue to be the preferred instrument for specifying regulatory technical details.
- Revise Article 18(2) to **remove or narrowly define any ENISA "leading" role in standardisation development**, while keeping participation and expert input to European standardisation as a priority.
- **Utilize the improved European Standardisation System to accelerate timely delivery of standards** and enable systematic consideration of Common Specifications and of other rule-setters' specifications where appropriate, without creating a parallel standard-setter and diverging standards.

AVOIDING UNNECESSARY BARRIERS TO STANDARDISATION

Article 100(4)(a) provides that high-risk suppliers shall not be entitled to participate in the development, assessment, and consultation of or in decisions concerning European standards, European standardisation deliverables and common specifications in the area of cybersecurity. DIN recognises the legitimate objective of addressing serious non-technical supply-chain risks. However, **embedding a blanket exclusion of a whole stakeholder group risks undermining key foundations of the European Standardisation System**– openness, inclusiveness, transparency, consensus and technical merit – and may reduce technical quality and market acceptance. Any ban would conflict with the WTO Agreement on Technical Barriers to Trade and may also create practical uncertainty for European and international standardisation work where participation rules differ. In summary, a ban could weaken Europe's position in international standardisation and weaken the appeal of European standards.

Importantly, the **ESS's principles of transparency, openness, consensus, and inclusiveness exist precisely to guarantee the quality of standards.** This includes avoiding any content that could create a risk to cybersecurity. These principles also give ENISA and any official national cybersecurity organisation the opportunity to participate in standardisation. Should these mechanisms not suffice, the Commission could still deny the listing of any European Standard within the OJEU and ENISA could alternatively develop required technical specifications. DIN therefore believes that the CSA2 and the ESS are already sufficiently equipped to handle any non-technical risks.

DIN recommends:

- **Maintain openness as the default** for standardisation to protect inclusiveness, interoperability and the global uptake of European cybersecurity standards.
- **Delete the reference to standardisation in Article 100(4)(a)** to avoid a blanket prohibition on the participation within standardisation by actors from third countries.

RELYING ON HORIZONTAL RULES FOR CONFORMITY ASSESSMENT

The CSA2 contains detailed provisions on conformity assessment and the operation of the certification ecosystem in its Annex I. DIN's perspective is that core requirements for Conformity Assessment Bodies, impartiality, competence, and consistent processes, are already addressed by the EN ISO/IEC 17000-series standards. Moreover, the Commission recommends this series for rules for conformity assessment bodies and has actively fostered their development.[2] For product and service certification bodies, EN ISO/IEC 17065 is a key horizontal reference. Where the CSA2 adds detailed operational requirements in parallel, there is a risk of duplication, inconsistencies across sectors, and reduced coherence with the New Legislative Framework (NLF) approach.

To **avoid this unnecessary bureaucracy, DIN advocates a "horizontal-first" approach**: EU legislation, and therefore the **CSA2 as well, should reference established legislation for conformity assessment and established processes**, e.g. the Blue Guide, wherever possible and add only narrowly tailored cybersecurity-specific requirements where strictly necessary. To enable this, the revision of the NLF, that is currently undertaken as well, should also reflect relevant needs of the CSA2. This seems particularly appropriate, since one of the key aims of the NLF revision is to make it fit for the digital age. In addition, DIN supports maintaining ISO/CASCO as the focal point for conformity assessment standardisation, to preserve global coherence and avoid fragmentation through sector-by-sector reinvention.

DIN recommends:

- Continue to reference the **EN ISO/IEC 17000-series (as relevant) as the baseline for Conformity Assessment Bodies**, adding only limited cybersecurity-specific requirements where justified.
- **Avoid embedding detailed, sector-specific operational rules for certification bodies** in CSA2 where horizontal conformity assessment standards already cover these aspects.
- **Support ISO/CASCO as the primary forum for conformity assessment standardisation** to preserve coherence and international alignment.
- Include proposals from CSA2-needs within the ongoing NLF-revision

[2] C.f. COM 2022.

About DIN

DIN, the German Institute for Standardization, is the independent platform for standardization in Germany and worldwide. Together with industry, scientific institutions, public authorities and civil society as a whole, DIN plays a major role in identifying future areas for standardization. By helping to shape the green and digital transformation, DIN makes an important contribution towards solving current challenges and enables new technologies, products and processes to establish themselves on the market and in society. More than 40,000 experts from industry, research, consumer protection and the public sector bring their expertise to work on standardization projects managed by DIN. The results of these efforts are market-oriented standards and specifications that promote global trade, encouraging rationalization, quality assurance and environmental protection as well as improving security and communication. For more information, go to http://www.din.de/en.