Cybersecurity Act 2

Strengthening security and resilience without sacrificing competitiveness

The resilience of Europe as a business location is a top priority for the electrical and digital industry – it is a fundamental prerequisite for a strong and sovereign economy. The ZVEI adopts a holistic concept of security that goes beyond purely technical risks and takes geopolitical realities into account. A well-designed trusted supplier approach focused on core sectors of critical infrastructure can contribute to this.

However, companies can only compete successfully in the global market if they remain able to act and can manage their resources autonomously. This also requires easing the regulatory burden. In the area of cybersecurity, ZVEI member companies are confronted with a growing number of regulations, the cumulative complexity of which ties up scarce skilled workers, hinders investment, and inhibits innovation potential. With its proposal to revise Regulation (EU) 2019/881, known as Cybersecurity Act 2, the European Commission states that it aims to reduce this complexity. The ZVEI expressly welcomes this goal. However, as a 'new' regulation, CSA 2 is unlikely on its own to meet these ambitions. Substantial relief is only possible by adapting existing regulations – mainly Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA) – to make them suitable for industry. This draft proposal of CSA 2 does not yet lead to significant cost savings or a noticeable reduction in bureaucracy.

The ZVEI supports the change of course initiated by CSA 2 towards a broad concept of security at the EU level. At present, however, neither the proportionality required for industry-wide adoption nor a realistic consideration of operational and technical implementation realities are sufficiently apparent. To secure the support of the electrical and digital industry, the following measures are necessary:

- **Limit supply chain requirements to sectors of high criticality.** The Trusted ICT Supply Chain Framework should only apply to NIS2 Annex I sectors, not Annex II.
- **Define high-risk suppliers with pragmatic legal certainty.** High-risk suppliers must not be defined as all manufacturers in a third country; only entities that are explicitly designated as such should be included.
- **Bans only where alternatives are demonstrably available.** Before imposing a ban on use, installation, or integration of ICT components, a reliable and comprehensive assessment must be made as to whether viable alternative suppliers are available.
- **Do not impose the costs of mandatory replacement measures solely on industry.** If components need to be removed, financial compensation mechanisms are required for the companies affected.
- **Provide sufficient transition periods for phase-out.** Replacement obligations must follow realistic, plannable, and risk-based transition periods.
- **Build on existing standards instead of creating parallel certifications.** The European Cybersecurity Certification Framework (ECCF) must not lead to regulatory fragmentation; global standards should be used wherever possible.
- **No new "cyber posture" scheme for NIS2 entities.** Instead of an additional certification system, existing and proven evidence such as ISO 27001 or TISAX should be recognized.
- **Strengthen ENISA – but without additional fees.** ZVEI supports a strong ENISA. Any expansion of its role should be funded without imposing additional fees on industry.

Trusted supply chain rules where risk is highest

ZVEI supports a broader supply chain security approach that addresses both technical and non-technical risk factors to reduce critical dependencies and vulnerabilities. A well-designed trusted supplier approach, limited to the core of critical infrastructure and grounded in clear criteria, can strengthen the EU's technological sovereignty while safeguarding Europe as a competitive business location.

Pragmatism and legal certainty must guide this endeavour. High-risk suppliers must be limited to specifically designated entities under Article 103(7) and the entities they control. They must not automatically include all manufacturers from a country identified as a country posing cybersecurity concerns under Article 100. Article 2(39a) is therefore misleading and should be revised accordingly. The relevant companies should be defined exclusively in Article 2(39b) as entities designated under Article 103(7) and the entities they control.

The current approach to ICT supply chain security focuses primarily on negative designations and restrictive measures. To provide greater legal certainty and further clarity, lawmakers should also consider the inclusion of a trusted partner clause. Such a clause could create a possibility to recognise partners whose governance and security systems are structurally aligned with those of the Union. In this context, a future "trusted partner country" regime could be factored into Union risk assessments. Companies or suppliers established in such trusted partner countries should not be exempt from scrutiny, but they could be treated as presenting a lower baseline risk. This would allow competent authorities and affected entities to focus more strongly on the technical evidence and the concrete risks of individual products or suppliers, rather than on geopolitical considerations alone.

To uphold the principle of proportionality and ensure the framework's feasibility and acceptance, the scope of the Trusted ICT supply chain framework must be limited to sectors of high criticality listed in Annex I of the NIS2 Directive. Accordingly, any ban on the use of ICT components from high-risk suppliers in ICT key assets, as well as any obligation to implement alternative mitigation measures, should apply only to entities in the energy, transport, finance, healthcare, water, digital infrastructure, public administration, and space sectors. This would align CSA 2 with the structural logic of the NIS2 Directive, which already distinguishes between sectors based on their risk profile and escalation potential. By focusing on the highly critical sectors listed in Annex I, CSA 2 would target the backbone of modern society, where disruption could trigger immediate systemic risks and cascading effects across other sectors. This risk-based, pragmatic approach is also reflected in the German implementation of the NIS2 Directive, whereby the use of so-called critical components in critical facilities (KRITIS) can be prohibited by the Ministry of the Interior, considering non-technical risk factors. EU-level regulation should follow the same logic.

A ban on the use, installation, and integration of ICT components from high-risk suppliers beyond these sectors of high criticality would, depending on its design, have far-reaching implications for the European economy, the full extent of which is difficult to quantify. What is clear, however, is that while the balance between administrative effort and resilience gains may still justify such an approach in Annex I sectors, extending it to Annex II sectors would impose costs that clearly outweigh the additional security benefits. In-depth analyses and ongoing monitoring of complex international supply chains and key ICT assets, as well as verifying whether they contain ICT components from high-risk suppliers, tie up scarce resources, require extensive documentation, and weaken competitiveness. This burden must be limited to sectors of high criticality.

The CSA 2 must be implemented with sufficient pragmatism to remain manageable for companies in the highly critical sectors listed in Annex I to the NIS2 Directive. The phase-out of installed components can only be an ultima ratio, to be applied based on a risk-based assessment and solely where no other suitable and more proportionate technical measures are effective in adequately mitigating the identified IT and cyber risks. Furthermore, the requirement that any ban on use, installation, and integration be preceded by a robust and reliable assessment of the availability of viable alternatives to high-risk suppliers must be applied strictly. Such a ban should only be imposed where that assessment clearly confirms that suitable alternative suppliers are available.

Should such bans be imposed, affected companies that have integrated components from high-risk suppliers into their ICT key assets cannot be left to bear the resulting administrative and financial burdens alone. Strengthening security and resilience is a responsibility shared by society as a whole. New ICT supply chain security regulations may compel EU companies from certain sectors to remove components from high-risk suppliers at costs reaching millions of euros per company. These expenditures serve broader societal security goals rather than direct business interests, thereby placing affected companies at a competitive

disadvantage in both EU and global markets. Financial compensation mechanisms should therefore be put in place to offset these publicly motivated costs.

Sufficient, realistic, and predictable transition periods for the phase-out of components from high-risk suppliers are essential. A ban on use, installation, or integration must not take effect abruptly in existing infrastructures. Transition periods must be based on the criticality of the ICT key assets concerned, the availability of technically and economically viable alternatives, and actual procurement and investment cycles.

Build on existing standards instead of creating parallel schemes

A competitive European industry depends on global standards. Against this backdrop, ZVEI takes a critical view of the expansion of the European Cybersecurity Certification Framework (ECCF). We see the danger of regulatory fragmentation not only within the European single market, but also increasingly at global level. Products and components should not have to be redesigned or recertified for different markets. Where available, internationally recognised standards should be used.

ZVEI welcomes that the CSA 2 proposal includes, in Article 87, a mechanism for the international recognition of European cybersecurity certificates and, vice versa, of equivalent third-country certificates. However, greater flexibility would be welcomed. Certifications from trusted partner countries whose governance and security systems are structurally aligned with those of the Union should benefit from a streamlined recognition procedure based on existing technical alignment, instead of having to wait in every case for separate implementing acts to be adopted. In addition, where certifications from recognised international standardisation bodies provide the same level of security as a European scheme and overlap with its scope, companies should be able to apply for recognition of those certifications at the corresponding level within the EU framework. This would reduce duplication and support the use of existing internationally recognised standards without creating additional parallel certification structures.

In this context, we also reject the introduction of a scheme for the so-called cyber posture of NIS2 entities. Although harmonised implementation of risk management measures under the NIS2 Directive should be supported, this should be done by recognising ISO 27001 or TISAX. There is no need for a new cybersecurity certification scheme under the European Cybersecurity Certification Framework, as it poses the risk of duplicating existing and well-functioning mechanisms. Since Member States can make the use of certain certification schemes by essential and important entities mandatory, we see the risk that companies that already fulfil ISO 27001 or equivalent norms might also be required to obtain certification under the new ‘cyber posture of entities’ certification scheme. This would create additional administrative burdens without improving the cyber resilience of those entities.

Strengthen ENISA’s role – not the cost burden on industry

Cybersecurity must be viewed from a transnational perspective, and a European cybersecurity authority with strong resources and capabilities is a key step towards European resilience. The electrical and digital industry welcomes the clear designation of ENISA as the EU’s centre of expertise for cybersecurity. Products from ZVEI members are used in all critical sectors and are essential for the smooth functioning of modern societies. Greater information-sharing through ENISA, the provision of verified and reliable cyber threat intelligence, and support for market surveillance under the CRA are therefore welcomed and should be implemented as part of continuous public-private cooperation. Guidelines must be developed in close cooperation with industry and must identify concrete, verifiable implementation paths for complex realities such as system extensions, mixed architectures, and critical sectors. The objectives of ENISA (Article 4) should explicitly state that the authority is to coordinate relevant market surveillance throughout the EU and ensure a level playing field for all market participants.

ZVEI opposes extending ENISA’s mandate to draft technical specifications under Union harmonisation legislation in the field of cybersecurity. For existing cybersecurity legislation under the New Legislative Framework, the development of Harmonised Standards should remain with the European Standardisation Organisations under Regulation (EU) No 1025/2012. ENISA may support the Commission with technical expertise and in the assessment of draft harmonised standards, but it should not assume a quasi-standard-setting role. This is all the more important because the Cyber Resilience Act already provides for Common

Specifications as a fallback mechanism where harmonised standards are not available, are not delivered in time, or do not satisfy the Commission request.

ZVEI opposes the introduction of ENISA fees. The fee mechanisms proposed in Articles 46 and 47 of the CSA introduce a cost recovery model to partially finance ENISA's budget. Under these provisions, manufacturers and conformity assessment bodies would be required to pay fees for participation in European certification schemes, for the issuance of certificates, and for technical testing tools provided by ENISA. This places an additional financial burden on companies and conformity assessment bodies, while the scale of that burden remains unclear, making compliance costs difficult to predict. Such fees should therefore not be introduced. Cybersecurity certification serves an important policy objective and should be financed from public funds rather than through additional and uncertain charges on industry. A fee-free framework would maximise the impact of ENISA's work, lower barriers to compliance, and help ensure a level playing field without penalising companies for contributing to higher cybersecurity standards.

Contact
Lennard Kreißl • Manager Digital Policy (Focus Cybersecurity) • Division Digitalisation & Law • Digital and Innovation Policy Department
Phone: +49 30 306960-582 • Mobile: +49 162 2664-941 • E-Mail: lennard.kreissl@zvei.org

Imprint
ZVEI e. V. • Electro and Digital Industry Association • Charlottenstr. 35/36 • 10117 Berlin
Lobby register no.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org

Date: 28.04.2026