Brussels, 26 June 2026

Cybersecurity Act 2: Recommendations to Deliver Resilience and Competitiveness

Executive summary

Orgalim welcomes the reinforcement of ENISA's mandate, improvements to the European Cybersecurity Certification Framework and the mitigation of non-technical risks in critical ICT supply chains.

1. Expansion of ENISA`s mandate: focus on added value

- Limit the expansion of ENISA's mandate and avoid the set-up of a parallel standard-setting organisation.
- Ensure adequate public funding for ENISA to develop and operate a secure a Single-Entry Point.
- Strengthen ENISA's role in interoperability across Member States, including coordinating market surveillance.
- Develop implementation guidelines in close cooperation with industry, addressing complex system realities.
- Maintain free participation for manufacturers in European cybersecurity certification schemes.

2. Targeted improvements to the European Cybersecurity Certification Framework (ECCF)

- Streamline the development of certification schemes
- Ensure certification schemes are voluntary, based on international or European consensus-based standards.
- Align the cyber posture certification scheme with existing international and European frameworks, grant presumption of conformity with NIS2, and replace national certifications.
- Organise structured and early industry involvement in scheme development.
- Develop a new certification scheme covering industrial products, systems, processes and services.

3. ICT supply chain security: clarify the criteria and methodology for designating high-risk suppliers

- Limiting high-risk designation to ensure proportionate mitigation of non-technical risks and avoid country-based designation.
- Restrict the Trusted ICT Supply Chain Framework scope to high-criticality sectors (Annex I of NIS2 Directive).
- Introduce procedural safeguards before bans or restrictive measures.
- Consider proportionate financial compensation mechanisms.
- Ensure structured stakeholder consultation during risk assessments.
- Provide realistic phase-out periods, particularly for final products already placed on the market.

Introduction

A targeted revision of the Cybersecurity Act (CSA) is essential to strengthen Europe's cyber reslience and ensure that the EU's cybersecurity framework remains fit for purpose, effective, coherent and aligned with the rapidly evolving technological landscape.

The revision must avoid an overly prescriptive approach that would increase regulatory complexity and could undermine industrial competitiveness – putting the global integration of European supply chains at risk. Orgalim therefore calls for close involvement of industry in the development of the Cybersecurity Act 2 and a proportionate approach that limits the negative implications for Europe's technology industries.

I. Expansion of ENISA`s mandate: focus on added value

Orgalim welcomes the reinforcement of ENISA's mandate and its designation as a European "centre of expertise on cybersecurity"[1] with appropriate resources and capabilities to support this role. Greater information-sharing through ENISA, the provision of verified and reliable cyber threat intelligence, and support for market surveillance are therefore welcome and should be implemented as part of a broader continuous public-private cooperation.

Orgalim recommends:

- **ENISA's new responsibilitiesshould complement and not replace its existing activities**. ENISA's expanded role in certification, standardisation and risk assessment should not dilute its focus on its core operational and advisory functions.

- **ENISA must not act as a parallel standard-setting body or regulatory authority.** . ENISA's role should be limited to providing technical expertise and coordination support to Member States and industry stakehoders. Orgalim warns against the expansion of ENISA`s role as a parallel European standardisation body (ESO) as the proliferation of ESOs would dilute the ability of industry to provide valuable input. Given the shortage of experts in the standardisation field, requiring expert involvement on drafting of standards or technical specifications through the consultation of the European Cybersecurity Certification Assembly would further strain already limited resources. ENISA`s role should be limited to assisting with the assessment of draft standards and the CSA2 should confirm that leadership and formal development of standards remain with the established ESOs. **The development of binding technical specifications should be treated as a fallback solution** and should not undermine the current public-private partnership. The expertise necessary to prepare the required specifications and to safeguard their acceptance already exists in CEN, CENELEC, and ETSI. Any system trying to achieve the same level of expertise, openness and transparency will inevitably create a parallel structure.

- **Participation in European cybersecurity certification schemes should remain free of charge for manufacturers**. The new fee mechanisms under Articles 46 and 47 could lead to additional direct and indirect costs for manufacturers. There should be no added fees for manufacturers for the issuance of certificates or for technical testing tools provided by ENISA as a result of the cost recovery model to partially finance ENISA's budget. While Orgalim recognises the need for sustainable funding to support ENISA's activities, cybersecurity certifications serve a public policy objective and should not impose new or uncertain financial burdens on technology providers, as this may increase compliance costs and discourage participation in European certification schemesA 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 that contribute to higher cybersecurity standards.

[1] Proposal for a regulation on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

- **ENISA should be adequately funded to develop and maintain the Single Entry Point,** as presented in the Digital Omnibus[2], in a reliable and secure manner. The Single Entry Point is a key simplification tool for companies when reporting incidents, provided it is set up to reduce the administrative burden.

- **ENISA's mandate should focus more on convergence and interoperability across Member States**, particularly in areas where fragmented national approaches create significant challenges for industry (e.g. approaches to risk management measures, certification, vulnerability handling, incident reporting etc.). **Article 4 should explicitly include ENISA's responsibility for coordinating relevant market surveillance across the EU**, in order to ensure consistent enforcement and a level playing field for all market participants.

- **ENISA should develop guidelines in close cooperation with industry** with the aim of identifying concrete, verifiable implementation paths for complex realities such as system extensions, mixed architectures and critical sectors.

II. Targeted improvements to the European Cybersecurity Certification Framework (ECCF)

European Cybersecurity Certification Schemes can be an important tool for harmonising requirements across Member States and strengthening trust in the single market. Since the adoption of the CSA, however, the development and finalisation of these schemes has progressed slowly. In this context, streamlining the procedure for developing certification schemes with a focus on technical security objectives and setting clear timelines are necessary improvements. Moreover, the proposed extension of the scope to include ICT processes, together with the possibility for certification schemes to serve as a presumption of conformity under relevant Union legislation, will further contribute to their added value and incentivise wider adoption by industry.

Orgalim recommends:

- **The cyber posture certification scheme should be developed in full alignment with existing international and European frameworks** (e.g. ISO/IEC 27001 standard, NIST Cybersecurity Framework, CyberFundamentals Framework, ENISA`s NIS2 Technical Implementation Guidance). The certification scheme should offer presumption of conformity with NIS2 and replace national-level certifications. In the interim, mutual recognition of existing audits should be permitted.

- **Certificates should remain voluntary in nature**. Orgalim particularly opposes any mandatory use of certifications under the NIS2 and CRA. A voluntary approach allows organisations to choose the compliance pathway that best fits their size, sector and risk profile, ensuring that certification is adopted where it offers clear added value. It will also avoid creating duplicative obligations for companies that already adhere to well-established standards and operate under existing assurance schemes that support compliance with the NIS2 Directive. If Member States can designate schemes as mandatory, companies could face an additional administrative burden without a corresponding security benefit. This should be reflected in the CSA2 as well as in the proposed targeted amendments to the NIS2 Directive. In addition, to enhance their added value and incentivise wider adoption by industry, **certifications should be based on international or European consensus-based standards**.

- **The development process of European Cybersecurity Certification Schemes should include further stakeholder consultation**. While Articles 74 and 75 of the CSA2 state that ENISA must consult stakeholders, more structured and meaningful involvement of industry representatives is necessary to ensure that schemes are practical and implementable. Since these schemes will ultimately be adopted and applied by industry, it is essential that the perspective of industry is integrated early and in a consistent manner.

2 Proposal for a regulation on amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)

- **The European Cybersecurity Certification Assembly should be set-up as a priority,** as it will provide an important opportunity for industry to share its insights on where certification brings added value and where efforts should be focused. In addition, Orgalim recommends that, in parallel, a dedicated industry stakeholder working group is established with a more structured and predictable engagement model than the current Stakeholder Cybersecurity Certification Group (SCCG). Under this approach, the European Cybersecurity Certification Assembly and the new stakeholder group should meet regularly to discuss progress on certification, exchange technical information, and ensure coherence throughout the development of schemes. The stakeholder group should have a clearly defined and meaningful role, including the ability to provide a formal non-binding opinion on candidate schemes.

- As it serves an important policy objective, **cybersecurity certification should be financed from public funds rather than through additional and uncertain fees levied on industry** (cf. to comments on fees in Articles 46 and 47 in the chapter above).

- The **set-up of a new voluntary certification scheme for industrial products, systems, processes, and services**:

  - There is currently no EU-wide cybersecurity certification framework that adequately reflects the specific risks, architectures and operational constraints of industrial contexts and critical infrastructure. European certification schemes should serve real market interests beyond compliance with EU regulations to boost the competitiveness of EU industry.

  - For this reason, the roadmap of the ECCF should include an industrial product, system, process and service certification scheme based on generally accepted international and European standards such as the IEC 62443 / EN IEC 62443 series. Anchoring certification schemes in widely-recognised international and European standards has a strong commercial interest, as it would allow companies to build on existing investments, facilitate market uptake, and support the global recognition of European industrial products – including exports to non-EU markets.

  - The ECCF should also establish a clear and coherent path from voluntary certification under CSA2 to compliance with the CRA, allowing companies that meet CRA requirements to demonstrate their maturity and create market differentiation through certification.

  - As part of development, prior, systematic market analysis and impact assessments (including analysing potential for international uptake) should be conducted to ensure schemes serve a real market interest.

III. ICT Supply chain security: clarify the criteria and methodology for designating high-risk suppliers

Orgalim supports the establishment of a harmonised EU-level trusted critical ICT supply chain framework to address systemic non-technical cyber risks, particularly in light of increasing geopolitical uncertainty and cross-border dependencies. The framework can provide a structured way to tackle ICT supply chain risks, identify high-risk suppliers or third country concerns, and apply proportionate mitigation measures or bans. The EU 5G toolbox fragmented implementation points to the necessity of a common solution to avoid further fragmentation and ensure a harmonised Union approach.

At the same time, it is equally **important that the implementation of the trusted ICT supply chain framework takes into account the operational and supply chain realities** faced by essential and important entities under the NIS2 Directive. Risk assessments and mitigation decisions must be realistic and technically feasible. Before any ban or restrictive measure is imposed, the availability of alternative suppliers, the maturity of the relevant alternative technologies and the criticality of the ICT asset in question must all be considered carefully. A one-size-fits-all approach can put at risk the system`s stability and business operations if technically equivalent or secure alternatives are not readily available. While carrying out such risk assessments, it is also essential to recognise that access to highly secure global IT solutions and cybersecurity services remains critical to safeguarding the EU's overall resilience.

Orgalim supports a wider approach to cybersecurity that goes beyond purely technical risks and takes into account the importance of mitigating non-technical risks in critical ICT supply chains. It is also important to consider the geopolitical realities of the EU's international partners such as Canada, the UK, Australia, Japan, India and the US, which have already implemented corresponding measures in critical supply chains similar to the CSA proposal of the European Commission. 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 manage their resources autonomously. This also requires regulatory simplification.

Orgalim supports the change of course initiated by the CSA2, complementing existing EU level technical cybersecurity architecture such as NIS2, DORA and CRA with EU-level binding instruments to address non-technical risks, thereby developing a broad concept of security at EU level. While doing so, it is essential to maintain proportionality and give due consideration to operational and technical implementation realities.

On designating high risk suppliers, Orgalim recommends:

- Clearly defining high-risk suppliers to ensure legal certainty. **High-risk suppliers must be limited to specifically designated entities under Article 103(7)** of the CSA2 and the entities they control. **Manufacturers should not be designated as high risk only because of their provenance from a country posing cybersecurity concerns under Article 100** of the CSA2. Article 2(39a) is therefore misleading and should be revised accordingly. The relevant companies should be defined exclusively in Article 2(39b) as an entity designated under Article 103(7) and the entities it controls.
- Limiting supply chain requirements to sectors of high criticality. **The Trusted ICT Supply Chain Framework should only apply to NIS2 Annex I sectors, excluding Annex II sectors**. This would align the CSA2 with the structural logic of the NIS2 Directive, which already distinguishes between sectors based on their risk profile and escalation potential.
- Implementing **safeguards to avoid misuse of political or individual interests and influences when prohibiting a supplier**. The decisions should be based on tangible evidence. 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. The **criteria and methodology for designating high-risk suppliers** should be established as follows:
    - The Commission, with the support of ENISA, should publish a harmonised, **EU-level methodology for assessing foreign ownership, control or influence (FOCI)**, including the criteria, evidence sources and weighting applied.
    - The CSA2 should **limit the concept of "control by a third country"** to clearly define and demonstrate situations of undue influence that pose a concrete security risk.
    - The CSA2 should **refrain from using nationality alone** as a proxy for assessing cybersecurity or supply chain risks.
- **Considering proportionate compensation.** Where regulatory requirements lead to the removal or replacement of certain components, it is important to consider the financial impact on affected companies. Emerging ICT supply chain security measures may require EU manufacturers to phase out components from suppliers designated as high risk, entailing substantial and unplanned costs. As these measures are primarily driven by public security objectives rather than company-specific risk decisions, they can have a material impact on competitiveness – particularly in global markets. It would be appropriate to consider proportionate compensation or support mechanisms for companies to help ensure that these broader policy objectives are achieved without disadvantaging European industry.

On the process of high-risk designation itself, Orgalim recommends:

- Implementing a **structured consultation mechanism** with relevant entities under the NIS2 Directive within the processes covered by Article 99 (security risk assessment), Article 102 (identification of key ICT assets), and Article 104 (identification of high-risk suppliers) of the CSA2.
- Ensuring that, while Member States and the Commission may require entities to adopt appropriate mitigation measures under Article 103(2), **the choice of which exact measures are implemented remains with the entity**. The effectiveness and adequacy of the chosen implementation should remain subject to oversight by the competent authorities.
- Establishing **realistic phase-out/transition timelines**. Adjusting supply chains for complex industrial technologies, particularly where requirements affect final products already placed on the market and their retrofitting, or the replacement of ICT components integrated into such products, is a lengthy and technically demanding process. It involves engineering changes, certification adaptations, procurement cycles, and alignment across extensive value chains. Where phase-out or replacement requirements apply, manufacturers should not be expected to assume responsibility for tracking, monitoring, or retroactively replacing individual components once products are in use. Replacement obligations must not take effect abruptly. Realistic, plannable, and risk-based transition periods are necessary. 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.

Orgalim aisbl
Arts 56
Avenue des Arts 56,
1000 Brussels, Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438