EUCC ISAC's Contribution to CSA 2 Public Consultation

Topic: Maintenance Framework and Role of ISACs in European Cybersecurity Certification Schemes

The EUCC ISAC is a stakeholder platform bringing together **industry experts, National Cybersecurity Certification Authorities (NCCAs), Conformity Assessment Bodies (CABs), and Certification Bodies (CBs)** to support the implementation and maintenance of the EUCC certification scheme. Through consolidated technical feedback and operational expertise, it plays an active role in ensuring the scheme remains effective, relevant, and aligned with real-world cybersecurity needs.

The EUCC ISAC strongly supports the overall objectives of strengthening the effectiveness, responsiveness, and long-term sustainability of European cybersecurity certification schemes. In this context, a robust, agile, and inclusive maintenance framework is essential to ensure that schemes continuously reflect evolving threats, technologies, and operational realities.

1. Support for Maintenance Governance and Technical Specifications

EUCC ISAC strongly supports the proposed maintenance governance model, in particular the reinforced role of ENISA in ensuring the continuous and effective update of certification schemes. The approach reflected in Article 77 on technical specifications represents a key improvement in this regard.

Allowing ENISA to develop, adopt and update technical specifications, and to publish them on its website, provides a level of flexibility and responsiveness that cannot be achieved through implementing acts alone. At the same time, the possibility to restrict access to certain sensitive elements, such as EUCC attack catalogues, ensures that security considerations are adequately addressed.

This model enables a more dynamic maintenance system, where technical content can evolve in line with emerging threats and operational feedback, while the core regulatory framework remains stable. EUCC ISAC therefore considers Article 77 to be a central element of an effective and future-proof certification framework.

2. Importance of Maintenance and Stakeholder Involvement

The credibility and effectiveness of European cybersecurity certification schemes depend on their ability to be continuously maintained and updated in a timely and robust manner. This includes ensuring that scheme documentation remains **at the state of the art**, reflecting the latest technological developments, threat landscape, and operational practices.

Stakeholder involvement is therefore a prerequisite for effective maintenance. Without such a structured engagement, certification schemes risk becoming disconnected from operational realities, reducing both their relevance and their uptake in the market.

3. Role of ISACs

Information Sharing and Analysis Centres (ISACs) provide a unique and indispensable contribution in this context. By aggregating expertise across sectors, value chains, representatives from public and private organisations, they deliver consolidated technical input and identify implementation challenges.

They also facilitate trusted information exchange between industry and public authorities, which is essential for ensuring that certification schemes remain aligned with real-world cybersecurity needs. While Recital 90 already recognises the potential contribution of ISACs, this recognition should be translated into clear and operational provisions within the legal framework.

4. Targeted Amendments to Article 75 and Expected Impact

EUCC ISAC considers that Article 75 on the maintenance of European cybersecurity certification schemes should be clarified and strengthened to ensure that stakeholder involvement is explicitly recognised and effectively implemented in practice, and that it fully gives effect to the intentions set out in Recital 90.

In particular, the framework should ensure **that ENISA systematically cooperates with relevant stakeholder groups, including ISACs**, and that stakeholder interaction is embedded as a core component of maintenance activities. ENISA should be able to organise structured engagement mechanisms, such as ad hoc working groups or sectoral liaison arrangements, where necessary.

At the same time, **ENISA should also be able to rely on existing and well-functioning stakeholder ecosystems, including ISACs**, which already provide consolidated expertise and established cooperation frameworks. Any new mechanisms should therefore build on and complement these existing structures, rather than duplicating, bypassing, or undermining them. In particular, the role of the EUCC ISAC as a functioning and trusted platform should be preserved and actively leveraged.

Furthermore, where maintenance activities or the development of new schemes are conducted through ENISA's ad hoc working groups, the process **shall include intermediary consultation steps prior to the finalisation of schemes or maintenance documents**. This is essential to ensure transparency and inclusiveness, and to prevent "black box" processes in which technical discussions are confined to a limited group of participants.

Taken together, these targeted amendments would significantly enhance the technical quality, responsiveness, and usability of certification schemes. They would strengthen trust among stakeholders, improve information flows between operational communities and public authorities, and fully complement the more agile maintenance model enabled by Article 77.

5. Conclusion

EUCC ISAC supports a CSA 2 maintenance framework that is operational, inclusive, and grounded in real-world expertise, and strongly endorses the enhanced role of ENISA in developing technical specifications.

To be effective, this framework must ensure that stakeholder involvement is structured, transparent, and meaningful, that the role of ISACs is clearly recognised and operationalised, and that existing

ecosystems such as the EUCC ISAC are preserved and actively used. It must also guarantee intermediary consultation steps to prevent opaque or closed processes.

EUCC ISAC stands ready to continue contributing to the maintenance of European cybersecurity certification schemes and to support ENISA and the Commission in the implementation of this framework.

Annex - Proposed Amendment to Article 75 (CSA 2)

Article 75 – Maintenance of a European cybersecurity certification scheme

Amendment to Article 75(2)

Replace the second sentence with:

ENISA shall cooperate and exchange information with relevant Union entities and groups, as well as with relevant stakeholder groups, including, where appropriate, Information Sharing and Analysis Centres (ISACs), in relation to maintenance activities.

New Article 75(3) (reworded)

Replace paragraph 3 with:

3. For the purpose of ensuring effective and technically robust maintenance of a European cybersecurity certification scheme, ENISA may, in accordance with the maintenance strategy referred to in paragraph 1, organise the structured involvement of relevant stakeholders, including through ad hoc working groups or sectoral liaison arrangements with relevant stakeholder groups such as Information Sharing and Analysis Centres (ISACs), without prejudice to ENISA's responsibility for ensuring the maintenance of the scheme.

Amendment to Article 75(4)(c)

Replace point (c) with:

(c) interactions and, where relevant, the establishment of liaisons with relevant stakeholders, including European or international standardisation organisations and Information Sharing and Analysis Centres (ISACs), including for the purpose of making or receiving technical contributions.