EU Cybersecurity Act's revision – call for evidence

EUCC ISAC feedback

The **EUCC Information Sharing and Analysis Centre (ISAC)** demonstrates a proven and trusted model of successful collaboration between public and private stakeholders. To ensure the continued relevance, trustworthiness, and effectiveness of cybersecurity certification schemes under the Cybersecurity Act (CSA), the revision should institutionalise this collaborative approach through structured mechanisms, notably through **Public-Private Partnerships (PPPs) supporting the ISAC model**.

1. Institutionalisation of the ECCG Subgroups for Scheme Maintenance and its liaison with private stakeholders

The **European Cybersecurity Certification Group (ECCG)** plays a critical role in the governance of certification schemes. To enhance its capacity for continuous maintenance and update of certification schemes:

- **Formalise dedicated ECCG subgroups** responsible for the maintenance and evolution of individual certification schemes.
- Ensure these subgroups are composed of **Member State representatives** and closely collaborate with technical expertise from relevant public and private stakeholders.
- Amend the CSA to require the **annual preparation and publication of a roadmap**, identifying documents to be reviewed and updated. This roadmap should be developed through structured **stakeholder consultations**.
- Reference models, such as the one provided by the EUCC ISAC maintenance model and its steering committee composed by public and private actors could serve as a foundation for defining maintenance best practices.

2. Strengthening ISAC as Technical Expertise Providers for Schemes' maintenance

The **EUCC ISAC** offers a well-functioning and agile structure for information sharing and technical expertise among Certification Bodies (CABs), vendors, schemes' users and public authorities. The **EUCC ISAC model** provides a trusted contributor structure, gathering the right level of expertise and trustworthiness between experts from private and public organisations. Moreover, this kind of structure ensures a Fair, Reasonable And Non-Discriminatory (FRAND) approach amongst its members while respecting antitrust rules and applying strict requirements related to Intellectual Property Rights (IPR) disclosure and essential patents.

The CSA revision should **recognise and formalise the role of ISACs**, particularly the EUCC ISAC, as **technical contributors** in the maintenance process of the EUCC scheme.

- ISACs provide rapid, industry-, vendor-, user-, and CAB-driven insights and should work **in close collaboration with ECCG subgroups representatives**.

- This collaboration could be structured though **formal contractual Public-Private Partnerships (cPPPs)**, enabling effective integration of technical expertise coming from private organization and industry into the regulatory maintenance framework, while preserving the ECCG's decision-making authority over maintenance oversight.

In contrast, the European Standardisation Organisations (ESO) model is not well-suited for scheme maintenance. By design, its structure does not rely on a trust-based framework among members. It typically allows broad participation without a qualitative selection process, involving individuals with varying levels of expertise—many of whom may not be directly aligned with the specific requirements of scheme upkeep. For example, activities such as penetration testing for level high or the maintenance of attack catalogues and quotation of attacks may fall outside the direct scope. This can result in a more prolonged and complex maintenance process, with an increased risk of sensitive document dissemination.

3. Establishing contractual Public-Private Partnerships (cPPPs) for Scheme Maintenance

To ensure the effective and sustainable maintenance of the EUCC scheme—and future European cybersecurity certification schemes—a structured PPP model should be established. This cPPP would consist in formal, structured collaboration between public authorities and private-sector stakeholders, established through formal agreements, bringing together regulatory bodies, national authorities, industry actors and relevant stakeholders to jointly support the maintenance, development, and continuous improvement of certification schemes and in particular the EUCC:

- This model incorporates rapid feedback loops from real-world deployments, enabling timely updates to certification schemes. For instance, the **EUCC ISAC Steering Committee** could serve as the core governance body for the cPPP for the EUCC maintenance. This committee would oversee the operational and technical contributions to the maintenance and evolution of the scheme, ensuring coordination across all relevant actors and ISAC technical groups.
- This committee should be composed of **National Cybersecurity Certification Authorities (NCCAs)** and **designated stakeholder representatives** from the private sector (e.g., vendors, CABs, industry associations). It would ensure a diversity of perspectives and expertise.
- The cPPP should ensure a **balanced, transparent, and inclusive** process for updating and evolving certification schemes, benefiting from the agility and expertise of the private sector while maintaining public trust and alignment with EU strategic objectives.
- Preservation of Public Oversight: while the cPPP allows for greater technical input and responsiveness, ultimate decision-making authority and regulatory oversight would remain with the ECCG and competent public authorities. This ensures that public trust, accountability, in the EU cybersecurity governance are maintained.