EUROSMART
The Voice of the Digital Security Industry

EUCS and the Future of Cloud Certification: Bridging Technical and Legal Gaps in the CSA

The European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) represents a critical step toward establishing digital sovereignty, trust, and resilience across Europe. However, the current version of the Cybersecurity Act (CSA) lacks several essential provisions needed to enable a robust EUCS scheme—particularly the inclusion of the so-called "High+" assurance level.

The ongoing revision of the CSA offers a timely opportunity to broaden the scope of the European Cybersecurity Certification Framework by integrating elements necessary to address an evolving and complex cybersecurity risk landscape. In particular, the CSA must allow certification schemes to incorporate non-technical requirements that are essential to a comprehensive cybersecurity approach.

Eurosmart therefore proposes targeted revisions to Article 54 of the CSA to ensure that the EUCS scheme is fit for purpose and fully aligned with European regulatory, strategic, and security priorities.

1. Inclusion of Non-Technical Requirements[1]

While technical robustness remains the core business of the CSA, cloud security also hinges on governance, jurisdictional alignment, and legal protections. To that end, the CSA should explicitly allow non-technical requirements in certification schemes, especially for high-assurance levels. The following aspects should be incorporated into the CSA revision to facilitate the finalisation of a robust EUCS scheme capable of protecting personal and sensitive data.

1.1. Immunity Requirements (necessary for the High+ Level)

Certificate applicants should demonstrate immunity from non-EU laws (e.g., the U.S. CLOUD Act) that could compel access to or disclosure of EU citizens' data. This requirement should apply

[1] See the exhaustive Eurosmart position paper on EUCS « High+ » requirements : European Cybersecurity certification scheme for Cloud Services and compatibility with EU regulations – what is missing? (April 2025)

at the proposed "High+" assurance level of the EUCS scheme, aligning with provisions in SecNumCloud and TS18026. This approach should be clearly defined and permitted by the CSA.

1.2. Data protection Requirements

Data - whether business or personal - is among the most valuable assets to protect in Europe, for the following reasons:

- **Privacy protection**: This entails the ability to demand full compliance with the GDPR for certified services, potentially extending obligations to legal entities as well as individuals.
- **Business competitiveness, continuity, and resilience**: This requires the protection of business-critical data, particularly information of high economic value or essential to operational continuity, as outlined in the European Data Act.

Data location requirements: It is essential to ensure that data storage, processing, and transmission occur within the EU or in third countries that provide equivalent legal safeguards. This requirement should cover all potential replication points, including Disaster Recovery sites and Content Delivery Networks (CDNs).

1.3. Legal Sovereignty

Certificates should also be able to reflect that services are governed solely by EU and national laws, with contracts subject to EU Member State jurisdiction. Compliance with legal sovereignty should be supported by traceable controls, as defined in TS18026 (e.g., CO-01.4H, ISP-02.2H, PM-04.8H).

2. Integration with Other EU Regulations

To streamline compliance and reduce regulatory fragmentation, the CSA should support EUCS certifications as a means of demonstrating alignment with:

- NIS2 Directive
- Digital Operational Resilience Act (DORA)
- Data Act
- General Data Protection Regulation (GDPR)

Certificates should provide "presumption of conformity" against the essential requirements of these laws, ideally managed through delegated acts under the CSA.

More generally when it comes to such cross-regulation compliance, mappings and analytical studies conducted by ENISA are crucial. Its missions in this respect should be enhanced. These efforts would significantly contribute to a more coherent and efficient European regulatory framework.

3. Qualification of Certified Entities

Inspired by the “SecNumCloud” model, the CSA should include a clearly defined qualification process to ensure that only entities with the necessary **trustworthiness**, **legal accountability**,

and **operational maturity** can access certification—particularly at higher assurance levels for service providers, such as the targeted "High+".

The CSA should clearly define this qualification process, which must include the following key safeguards:

STAGE	DESCRIPTION
EVALUATION	Certification candidates should undergo a comprehensive technical and organizational assessment conducted by **NCCA-accredited laboratories**. This includes both documentation reviews and on-site audits where applicable.
VALIDATION	Evaluation results must be independently reviewed by the **National Cybersecurity Certification Authority (NCCA)**. A certificate is granted only if all requirements are fully met.
MAINTENANCE	Once certified, entities should be subject to **ongoing compliance monitoring**, including **annual audits**, **incident reporting**, and **ad hoc re-evaluations** in case of significant changes or identified risks.

The qualification framework should also:

- **Define eligibility criteria**, including the legal status of the organization, its jurisdictional footprint, and its ability to comply with EU law.
- Require demonstration of **internal governance and security policies, data protection practices, and incident response procedures.**
- Include mechanisms for revocation or suspension of certification in case of serious non-compliance or operational failure.

Such a process strengthens the integrity and credibility of the EUCS by ensuring that certification is not only a technical label but a holistic indicator of reliability, accountability, and strategic alignment with EU values.

4. New domains that would benefit from European Cybersecurity Certification and Contribute to the EUCS efficiency.

Implementing a Secure Development Lifecycle (SDL) enables organizations to demonstrate that their internal development practices meet established security and compliance requirements. As part of the Cyber Resilience Act (CRA), product security must be addressed during both the design and operational phases. During the design phase, applying an SDL process and leveraging European cybersecurity certifications can support the demonstration of compliance.

Trusted supply chain and evaluators: Any third parties involved in supplying components, conducting audits, or participating in lifecycle maintenance should themselves be certified or verified by EU authorities. This extends the trust perimeter beyond the core service provider.

Together, these measures ensure that EUCS-certified services not only meet security benchmarks but also operate within a legally and operationally trustworthy environment, aligned with the EU's strategic autonomy objectives

Conclusion

To ensure that the EUCS scheme meets its strategic objectives, Eurosmart recommends the following enhancements to the CSA:

- **Inclusion of immunity, privacy, and legal sovereignty requirements**
- **Alignment with GDPR, DORA, NIS2, and the Data Act**
- **Qualification framework for certified entities**
- **Address SDL through the Union rolling work programme for European cybersecurity certification schemes**
- **Reuse and alignment with national schemes and already existing technical specifications such as TS18026**

These measures will establish the EUCS as a credible and future-proof instrument supporting European cybersecurity, digital autonomy, and legal clarity.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com