# Joint Statement on EUCS

We welcome the objective of establishing a minimum set of security and trust criteria for cloud services via certifications. However, the ongoing process of developing a cybersecurity certification scheme for cloud services (EUCS) has been raising serious concerns amongst the industry.

The drafting of EUCS should be a purely technical process detailing the technical requirements for cloud services certification. ENISA's current candidate scheme includes political and legal sovereignty elements such as the requirement to have the company's headquarters located in the EU, restrictions on ownership and governance restrictions.

As things stand today, the inclusion of such requirements will be a step back and will ultimately undermine real competition in the European market, reduce choice for cloud customers and harm European industry and citizens. However, such sovereignty requirements for critical third-party providers were rejected by political decision-makers when shaping the Digital Operational Resilience Act (DORA). DORA envisages instead a direct oversight regime for critical TPPs (including cloud service providers) instead of restrictions on non-EU technology providers.

The current EUCS text also includes broad, undefined concepts and terminology which leads to further uncertainty. For the highest level of assurance (CS-EL 4) which is applicable to cloud services processing data of "*particular sensitivity and the breach of which is likely to result in a breach of public order, public safety, human life or health, or the protection of intellectual property",* the term "particular sensitivity" is vague and open to different interpretations, raising questions on its applicability to financial services.

Moreover, while cybersecurity certifications schemes were introduced as voluntary by the Cybersecurity Act, various legal texts – whether already in force or still under development can allow authorities to make these certifications mandatory for CSPs that offer services to "critical infrastructure" like healthcare, postal services, financial services, and waste management.

Cloud adoption by financial services, which is steadily increasing, is key to improving agility, international competitiveness, capacity, resilience, client experience and cost efficiency, and even security. Depriving companies of a real choice of cloud providers will endanger their operational resilience and stifle digital innovation. The EU cloud market is at the moment unlikely to meet the demand in terms of quantity and quality putting financial services in a vulnerable position.

Furthermore, the lack of transparency in the process is also concerning. The last and only public consultation carried out on the draft certification scheme took place in 2021. Since then, the text has undergone significant changes, including the introduction of sovereignty requirements which had not been part of the consulted version. However, those changes have never been made officially available, undermining the trust in the process and the purpose of the requirements of the scheme certification. We believe that ENISA and the European Commission should:

- Remove the sovereignty requirements from the EUCS candidate scheme and adopt an implementing act which focuses purely on technical requirements that will strengthen the European internal market, as existing EU policies set out in DORA, GDPR and NIS2 provide the best tools for tackling operational resilience and oversight of ICT critical third-party providers; and
- Actively engage with the industry during this process to ensure that the final scheme is adequate and fit for purpose.

We would welcome the opportunity to further discuss this with you.