

Practical aspects of cybersecurity certification: The CUSTODES approach

<u>Custodes</u>: A Certification approach for dynamic, agile and reUSable assessmenT fOr composite systems of ICT proDucts, servicEs, and processeS

Professor Nineta Polemi <u>trustilio BV</u> nineta.polemi@trustilio.com

> Grant Agreement number: 101120779 — CUSTODES HORIZON-CL3-2022-CS-01-04







Certification

-<u>Cybersecurity Act</u> Regulation (EU) 2019/881 on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

-AI ACT: Conformity assessment (Article 43) compliance with the requirements set out in Section 2 (Articles 8-15), the provider has applied harmonised standards.



RISK MANAGEMENT VS CONFORMITY ASSESMENT

security requirements of the products (manufacturers)



Conformity Assessment uses of cybersecuirty scheme (a structured approach to be used for the assessment e.g. EUCC) to assess how the security requirements in the PPs are met (auditors)

Risk Management is essential for the development of the Protection Profile (PP). PPs define the



Conformity assessment based multi schemes













CUSTODES will develop and implement an innovative configurable, user-friendly and cost-effective **Composite Inspection and Certification (CIC) System** which will facilitate the cybersecurity certification of the Composite TOE (ICT Products, ICT Services, and ICT Processes), promote collaboration and information sharing and assist the various interested parties in the identification and implementation of the relevant assessment activities as needed in alignment with the relevant standards and technical specifications where applicable.





CUSTODES

Objective 1: Promote the scalable, agile and verifiable certification of Composite TOE, towards ensuring and fostering the protection, resilience of the ICT products, ICT services and ICT processes, converting Europe into a Trustworthy Certified Digital Ecosystem.

Objective 2: Facilitate the accurate definition, evaluation and classification of complex and highly interconnected (Composite) Targets of Evaluation (TOE)

Objective 3: Optimize, automate and facilitate the conformity assessment of Composite TOE ensuring compliance and mitigating potential compliance breaches.

Objective 4: Establish and guarantee the trust relationships in the Certification process.

Objective 5: Enable robustness and sustainability of the self-assessment (i.e. audit/testing) throughout TOE lifecycles

Objective 6: Promote and enable the trustable and transparent sharing and reuse of certification related information

Objective 7: Development, validation and demonstration of CIC System through its application to large-scale real scenarios/conditions - Market validation and Roll out

Objective 8: Provide tailored certification-related recommendations



CUSTODES Composite Inspection and Certification (CIC) System





Certification International, European or national Scheme 1 Standards and/or other technical 0 specification applied to the evaluation pection and Certification CIC) System 1. Split Composite Product into layers of composability (Building Blocks under evaluation) Conformity assessment based multi schemes 2. Evaluate cyber risks & threats in the context The security environment in which **Composite Target** the TOE is intended to be used of Evaluation (TOE) 3. Generate a risk treatment plan Dynamic Risk Assessment (RA) Component Security Profile 1 II the certification-related data, information and evidence are further converted to a common representation format Building Block scovery Multi Assurance nponent Evaluation Certificate / Declaration of Conformity **Composite Conformity Assessment Process** (CCAP) Component







Thank you!

Professor Nineta Polemi <u>trustilio BV</u> nineta.polemi@trustilio.com



Grant Agreement number: 101120779 — CUSTODES HORIZON-CL3-2022-CS-01-04







