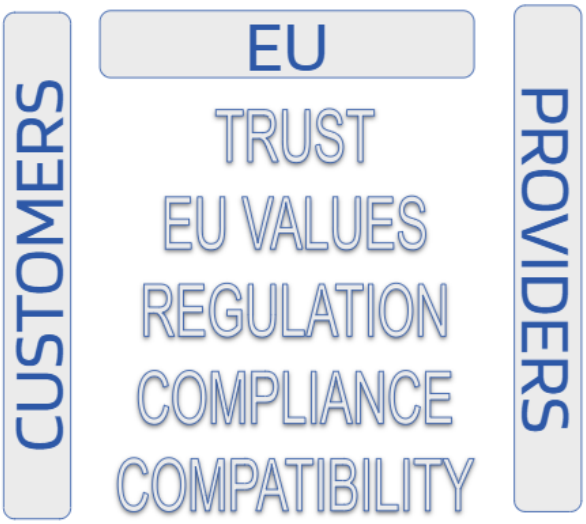
The DOME compliance policy

Being the DOME scope to create a framework supporting the market requirements, the definition of the policy starts from the definition of a baseline, **defining the minimum compliance level to ensure acceptability by the majority of the market sectors**. This definition is excluding by design any vertical requirement of a market sector or any enhanced qualification. Those second-level qualifications will be used to furtherly raise the qualification level of the offering but not to exclude something from the listing.

The scope is to ensure a reasonable level of compliance while minimizing the exclusions.



Aligning with the market the minimum compliance level is defined by Customers, while Providers have to commit to reach such compliance. The role of the DOME organization in this process is to balance the requirements of the Customer Base with the sustainability of the Providers. Too high requirements will land in poor offering because the Providers will not be able to sustain the costs related to the acquisition and the maintenance of such high compliance levels.

On the other side several other organizations are already working on the definition of a compliance level for cloud offering, and DOME will try to keep as much compatibility as possible with most of them in order to create the conditions for a future sharing of such visibilities between organizations.

In line with other established initiatives (i.e., Gaia-X) the DOME compliance policy is mapping the different criteria in different compliance levels according to the evidence provided by the offering vendor during or after the onboarding process.

Being DOME not committed to assess the delivery platform of every provider claiming to be listed on the DOME catalogue, the compliance policy is relying on complying with the criteria that have been selected as the main relevant ones for the trustability of the services in DOME.

Thus, the DOME compliance approach is designed to ensure that service providers meet rigorous quality standards, encompassing regulatory respect, data security, and service management best practices. This framework is based on a set of reference quality criteria that serve as the foundation for evaluating compliance.[1]

The validation of cybersecurity compliance for services in DOME is conducted through a manual assessment of cybersecurity controls , complemented by the transformation of digitally signed or unsigned document-based certificates and self-attestations into machine-readable compliance evidence in the form of Verified Credentials.

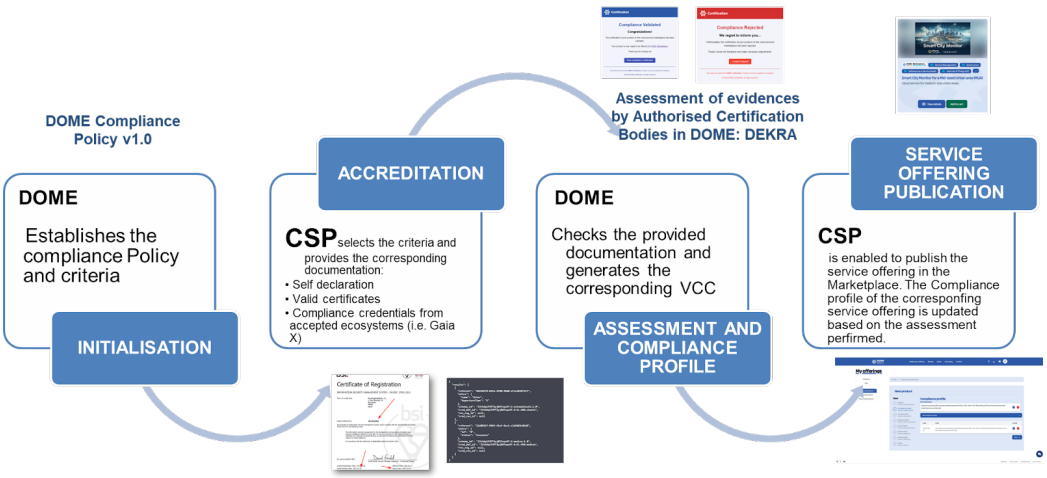
The main objectives of the compliance support in DOME are as follows:

- To establish a formal process for verifying compliance with reference cybersecurity controls
- To design a methodological framework, supported by tools, for assessing compliance with reference cybersecurity controls during the onboarding process
- To develop tools for the continuous monitoring of security requirements, ensuring ongoing compliance through the regular assessment of the validity of provided certificates and self-attestations

To this end, DOME ensures that services listed on the marketplace are certified by verifying the validity of the associated compliance documents through a structured three-step process:

1. Accreditation of the Compliance Profile: This phase involves the activities that Cloud Service Providers (CSPs) must undertake to provide the necessary information demonstrating compliance with the relevant criteria. It is integrated into the cloud service offering definition process.
2. Assessment and Endorsement: Once CSPs submit the required certificates or self-attestations, the DOME Trusted Service Provider for Certification (in the context of the project, this role is fulfilled by DEKRA, a member of the DOME consortium) evaluates the submitted documentation. If the assessment is successful, the Trusted Service Provider, through the Issuer, generates the corresponding Verified Credential for Certification (VCC) for the service within DOME.
3. Cloud Service Offering Publication: Upon issuance of the VCC, the CSP is able to publish its service offering in the DOME marketplace, accompanied by a valid and trusted compliance profile represented in the VCC.

It is important to note that DOME itself does not issue certifications. Instead, it relies on valid compliance documentation (either third-party-issued certificates or self-attestations) provided by the CSPs to ensure the compliance against the cybersecurity criteria.



[1] The DOME Compliance criteria has been defined based on the analysis of the Gaia-X Compliance criteria https://docs.gaia-x.eu/policy-rules-committee/compliance-document/24.11/criteria_cloud_services/#assessment-procedures and adapted to the needs of DOME

Revision #11
Created 7 December 2023 10:38:30
Updated 3 December 2025 12:19:59 by Juncal Alonso