

DOME Compliance policy v1.0

- [The DOME compliance policy](#)
- [Key Components of the DOME Compliance framework:](#)
- [Profile 0: Unmatching baseline requirements](#)
- [Profile Baseline: baseline eligibility criteria matched](#)
- [Profile Professional : Enhanced compliance](#)
- [Additional criteria and certifications](#)
- [How to check for a product qualification](#)
- [How to recover an expired qualification](#)
- [How to qualify a product \(User Guide\)](#)

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

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

Key Components of the DOME Compliance framework:

The DOME compliance framework is structured around three fundamental pillars, which have collectively shaped its foundation and definition

1. **Self-assessment:** Providers are required to issue a declaration attesting their compliance with the reference quality criteria after they have assessed themselves that they comply with them. This process encourages providers to take ownership of their compliance and ensures transparency.
2. **Certification Overlay:** Providers can supplement their self-declarations with official certifications that automatically assess compliance with specific subsets of the reference criteria. Multiple certifications can collectively cover the full range of requirements, reinforcing the validity of the compliance claims.
3. **Compliance Categorization:** Based on the level of compliance with the reference criteria, DOME assigns a Compliance Category to each offering. This categorization reflects the provider's adherence to the quality standards and is essential for the offering's visibility and status within the catalogue.

COMPLIANCE LEVELS

Currently, DOME has established three distinct compliance profile levels. These levels serve a dual purpose: (1) they set the minimum requirements for offers to be published in the DOME catalogue and (2) they establish a trust framework for providers, enabling them to transparently display their compliance posture, and allowing customers to make informed decisions when selecting cloud services that meet their trust requirements. To this end, DOME compliance levels have been defined as follows:

- **Baseline Compliance Level** : Offerings with self-assessed compliance that lacks formal certification are eligible for this level. They can be published in the catalogue with a baseline status, indicating a foundational level of compliance.
- **Professional and Professional + Compliance Levels** : Offerings with certified compliance evidence (valid certifications) are eligible for these levels. These levels signify a higher degree of compliance and trustworthiness, enhancing the offering's standing within the catalogue. Based on the type and number of valid certifications Professional or Professional + level can be achieved.
- **Non-Compliant Classification** : Offerings that fail to meet one or more mandatory compliance criteria, as determined through self-attestation or certification, are classified as non-compliant. Such offerings are excluded from the official catalogue, ensuring that only compliant services are presented to users.

CONTRACTUAL AND LEGAL IMPLICATIONS

The **compliance self-attestation** made by a provider is both legally and contractually binding with the DOME organization and is also a representation issued to potential buyers of the services. Any false or misleading declaration will result in immediate reclassification to a Non-Compliant status, disqualifying the provider and related offerings from catalogue visibility. From a legal perspective, this would amount to a misrepresentation that would expose the provider to potential legal claims from customers. This measure upholds the integrity of the compliance process and maintains the trustworthiness of the catalogue. The self-attestation mechanism is offering-specific, meaning that the declarations must be filled in from the perspective of each specific offering, not from the standpoint of the whole company. For instance, a cloud offering of a cloud service provider can provide portability and interoperability while another offering from the same provider does not. In that case the former would be eligible for publication in the DOME catalogue, while the latter would not.

The availability of **one or more official certifications**, issued by an official Certification Body, stating the profile of compliance with the defined criteria. Providers must provide such visibility (uploading the related documents or

digital credentials of the documents) during the offering publishing process.

All the certification documents must clearly state:

- The legal entity owning the certification
- The Certification Authority that issued the certification
- The validity period of the certification
- A statement allowing the capability to understand if the published service is covered by such certification or not (also known as “the scope” of the certification).

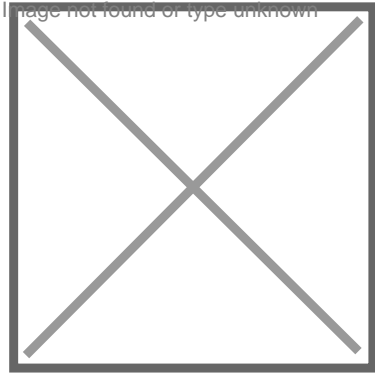
The lack of one or more of the above requirements may classify that evidence as unacceptable.

Profile 0: Unmatching baseline requirements

The product offering not matching the baseline qualification requirements are assigned a Level 0 label and not going to be shown on the shared catalogue. This qualification is usually applied to newly published products not yet verified by the DOME compliance unit.

IMPORTANT: The Level 0 classification avoids the replication of the offering through the catalogue and the visibility of the offering from the Customers browsing the catalogue.

Profile Baseline: baseline eligibility criteria matched



This is the entering acceptance level to enable offer visibility and sharing through the DOME ecosystem. To match this level the provider must provide visibility (through **self-attestations²**) of the implementation of the following **mandatory compliance criteria under the following categories:**

1- DATA PROTECTION AND MANAGEMENT

Criterion DP-1: The Provider shall offer the ability to establish a written contract under Union or EU/EEA/Member State law and specifically addressing GDPR requirements.

Criterion DP-2 : The Provider shall define in writing the roles and responsibilities attributed to each party in the offerings.

Criterion DP-3: For each offering, the Provider shall clearly define the technical and organizational measures in accordance with the roles and responsibilities of the parties, including an adequate level of detail.

Criterion DP-4: The Provider shall not access Customer Data unless authorized by the Customer or when the access is in accordance with applicable laws to the contract.

Criterion DP-5: The Provider offering is compliant with all the requirements of applicable laws and regulations concerning the protection of personal data, and specifically the General Data Protection Regulation (Regulation (EU) 2016/679).

2- CYBERSECURITY

Criterion CS-1: Organization of information security: Plan, implement, maintain and continuously improve the information security framework within the organisation.

Criterion CS-2: Information Security Policies: Implement adequate and updated information security policies and procedures aligned with the security requirements needed to support the Offering operational requirements.

Criterion CS-3: Risk Management: Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the Provider.

- Criterion CS-4:** Human Resources: Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination of employment contract.
- Criterion CS-5:** Asset Management: Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.
- Criterion CS-6:** Physical Security: Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.
- Criterion CS-7:** Operational Security: Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.
- Criterion CS-8:** Identity, Authentication and access control management: Limit access to information and information processing facilities.
- Criterion CS-9:** Cryptography and Key management: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.
- Criterion CS-10:** Communication Security: Ensure the protection of information in networks and the corresponding information processing systems.
- Criterion CS-11:** Portability and Interoperability: The provider shall provide a means by which a customer can obtain their stored customer data, and provide documentation on how (where appropriate, through documented API's) the customer can obtain the stored data at the end of the contractual relationship and shall document how the data will be securely deleted from the provider's system in what timeframe.
- Criterion CS-12:** Change and Configuration Management: Ensure that changes and configuration actions to information systems maintain an adequate security of the delivered cloud service.
- Criterion CS-13:** Development of Information systems: Ensure information security in the development cycle of information the concerned cloud offering.
- Criterion CS-14:** Procurement Management: Ensure the protection of information that suppliers of the provider can access and monitor the agreed services and security requirements.
- Criterion CS-15:** Incident Management: Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.
- Criterion CS-16:** Business Continuity: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.
- Criterion CS-17:** Compliance: Take positive and affirmative steps to ensure compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.
- Criterion CS-18:** Dealing with information requests from government agencies: Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of Customer Data.
- Criterion CS-19:** Offering's security: Provide appropriate mechanisms for cloud customers to enable Offering security. Ensure that the by-default configuration of the offerings is secure.

Profile Professional : Enhanced compliance



Following conditions are to be considered “on top” of the ones already described in Level -Baseline.

The “professional” profile is comprehensive and includes verified evidence (in form of certificates) that the different compliance criteria are being satisfied. These evidences need to be issued by authorized authorities and are validated by the DOME marketplace through the assessment of the trustability of the presented certifications. The process for the provision of the evidence (self attestation and certificates) is described in a separate document.

Currently the certifications that DOME can verify are:

- SecNumCloud
- BSI-C5
- CISPE
- EU Cloud CoC
- CSA CCM
- ISO/IEC 27001
- TISAX
- SWIPO

This list will be updated yearly in order to adapt these requirements to the new certification schemes that are developed in Europe.

CRITERIA	ACCEPTED CERTIFICATIONS
DATA PROTECTION AND MANAGEMENT	
DP-1, DP-2	SecNumCloud CISPE EU Cloud CoC

DP-3	SecNumCloud BSI-C5-Basic criteria CISPE EU Cloud CoC CSA CCM ISO/IEC 27001 TISAX
DP-4	CISPE EU Cloud CoC SecNumCloud BSI C5 CSA CCM
CYBERSECURITY	
CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, CS-8, CS-10, CS15	SecNumCloud BSI-C5 CISPE EU Cloud CoC CSA CCM ISO/IEC 27001 TISAX
CS-9, CS-17	SecNumCloud BSI-C5 EU Cloud CoC CSA CCM ISO/IEC 27001 TISAX
CS-11	SecNumCloud BSI-C5 EU Cloud CoC CSA CCM SWIPO IaaS TISAX
CS-12, CS-13; CS-14	SecNumCloud BSI-C5 EU Cloud CoC CSA CCM ISO/IEC 27001 TISAX
CS-16	SecNumCloud BSI-C5 EU Cloud CoC CSA CCM ISO/IEC 27001
CS-18	BSI-C5 EU Cloud CoC CSA CCM

CS-19	BSI-C5 EU Cloud CoC CISPE CSA CCM
--------------	--

Apart from the accreditations of the criteria mentioned above through the listed certifications, there are other criteria that need to **be self-assessed and attested by the provider to achieve the Professional level**:

CYBERSECURITY:

CS-20: User documentation: Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers.

PORTABILITY:

PT-1: The Provider shall implement practices for facilitating the switching of Providers and the porting of Customer Data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the Customer.

PT-2: The Provider shall ensure pre-contractual information exists, with sufficiently detailed, clear and transparent information regarding the processes of Customer Data portability, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another Provider or port Customer Data back to its own IT systems.

SUSTAINABILITY:

ST-1: The Provider shall provide transparency on the environmental impact of the Service Offering provided.

ST-2: The Provider shall ensure that the Service Offering meets or relies on an infrastructure Services Offering which meets a high standard in energy efficiency, meeting an annual target of PUE of 1.3 in cool climates and 1.4 in warm climates.

ST-3: The Provider shall ensure that the Service Offering meets or relies on an infrastructure for which electricity demand will be matched by 75% renewable energy or hourly carbon-free energy by 31st December 2025, and 100% by 31st December 2030.

ST-4: The Provider shall ensure that the Service Offering meets or relies on an infrastructure Services Offering that will meet a high standard for water conservation demonstrated through the application of a location and source sensitive water usage effectiveness (WUE) target of 0.4 L/kWh in areas with water stress.



These **additional criteria 7 criteria** can be also **accredited through related certificates** to achieve the compliance level **Professional +** that need to be verified by DOME:

CRITERIA	ACCEPTED CERTIFICATIONS
CYBERSECURITY	
CS-20	BSI C5 EU Cloud CISPE
PORTABILITY	
PT1	SecNumCloud SWIPO IaaS
PT2	SWIPO IaaS
SUSTAINABILITY	
ST1, ST2,ST3,ST4	CNDCP (Climate Neutral Data Centre Pact)

When **DOME verifies the compliance of the additional 7 criteria through the validation of the defined certificates** the service achieves the **Professional +** compliance level.

Additional criteria and certifications

Additionally, some other criteria and certifications will be accepted in DOME, although will not be required to achieve any level. These criteria (through self-attestation) or/and certifications will be visible in the offering compliance profile but won't have influence in the compliance levels.

EUROPEAN CONTROL

EC-1: The Provider shall provide the option that all Customer personal data are processed and stored exclusively in EU/EEA.

EC-2: The relevant offering shall process and store all Customer personal data exclusively in the EU/EEA.

EC-3: If the Provider or any of its subcontractors is subject to legal obligations to transmit or disclose Customer personal data on the basis of a non-EU/EEA statutory order, the Provider shall have verified safeguards in place to ensure that any access request is compliant with EU/EEA/Member State law.

EC-4: The Provider's registered head office, headquarters and main establishment shall be established in a Member State of the EU/EEA.

EC-5: The Provider's registered head office, headquarters and main establishment shall be established in a Member State of the EU/EEA. Shareholders in the Provider, whose registered head office, headquarters and main establishment are not established in a Member State of the EU/EEA shall not, directly or indirectly, individually or jointly, hold control of the provider. Control is defined as the ability of a natural or legal person to exercise decisive influence directly or indirectly on the CSP through one or more intermediate entities, de jure or de facto. (cf. Council Regulation No 139/2004 and Commission Consolidated Jurisdictional Notice under Council Regulation (EC) No 139/2004 for illustrations of decisive control).

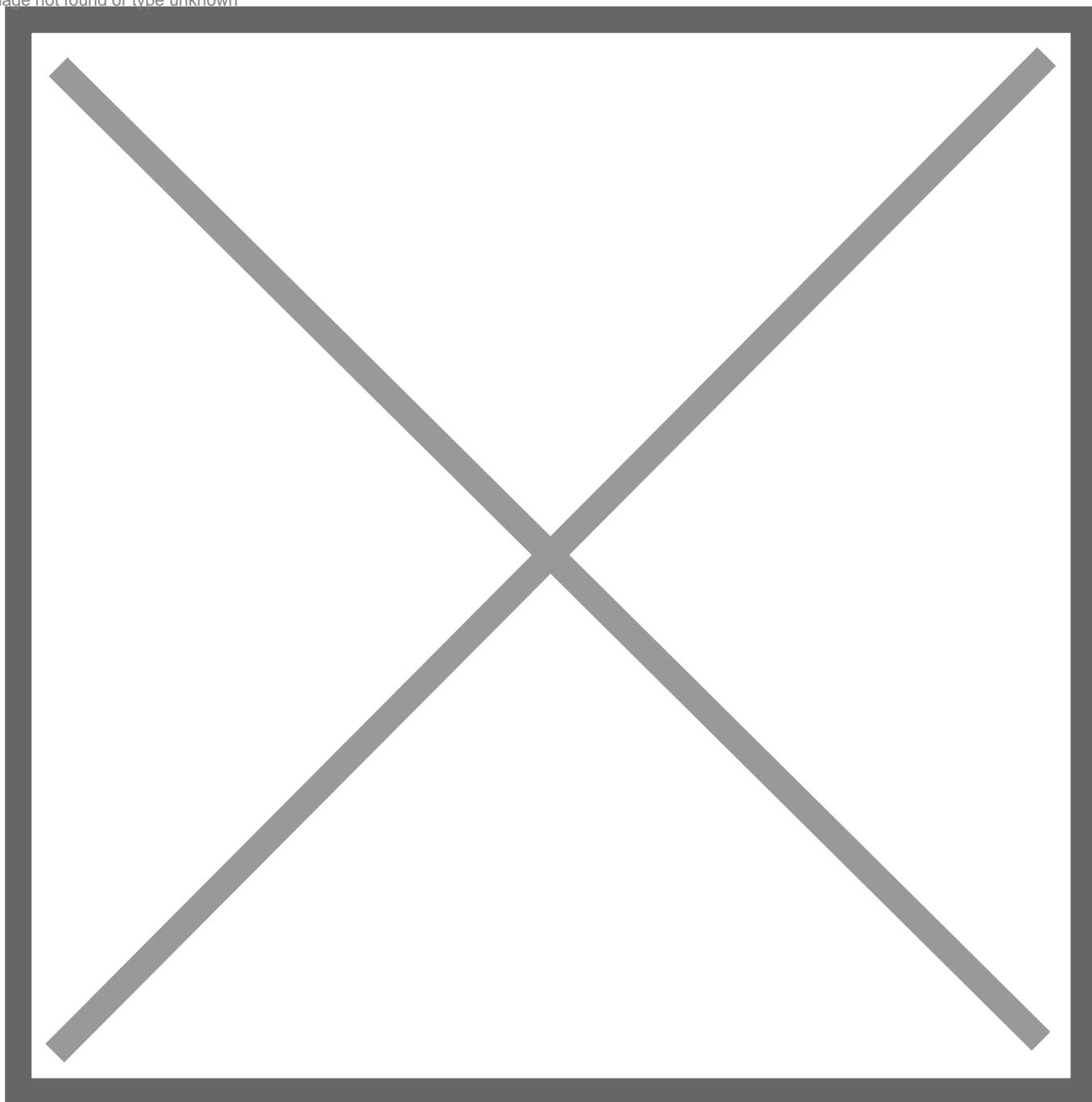
EC-6: In the event of recourse by the Provider, in the context of the services provided to the Customer, to the services of a third-party company - including a subcontractor - whose registered head office, headquarters and main establishment is outside of the European Union or who is owned or controlled directly or indirectly by another third-party company registered outside the EU/EEA, the third-party company shall have no access over the Customer personal data nor access and identity management for the services provided to the Customer. The Provider, including any of its sub-processors, shall push back any request received from non-European authorities to obtain communication of Customer personal data relating to European Customers, except if request is made in execution of a court judgment or order that is valid and compliant under Union law and applicable Member States law as provided by Article 48 GDPR.

EC-7: The Provider must maintain continuous operating autonomy for all or part of the services it provides. The concept of operating autonomy shall be understood as the ability to maintain the provision of the cloud computing service by drawing on the provider's own skills or by using adequate alternatives.

How to check for a product qualification

The information of the compliance profile will be available in the market place, including the DOME Compliance Level for each service.

Image not found or type unknown



To acquire more detailed information about the compliance profile 'view details' shall be clicked, and the detailed information will be shown . Check DOME certification baseline for the colour code.

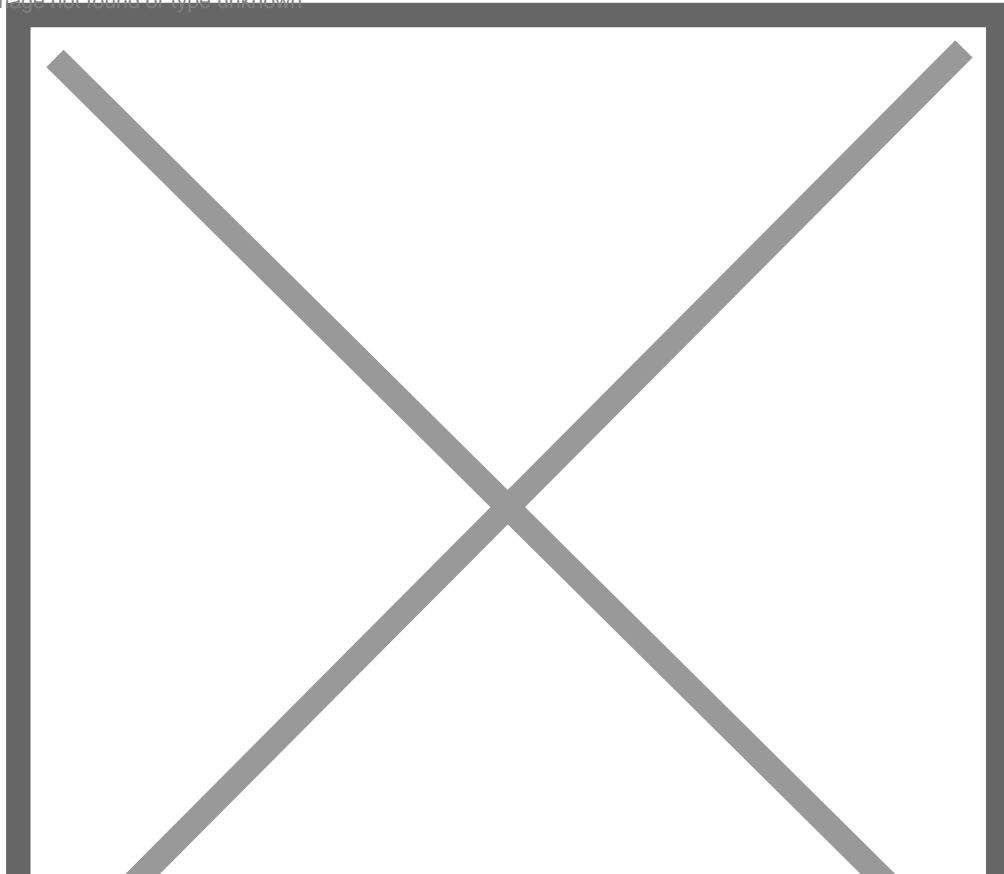
Image not found or type unknown

Image.png

How to recover an expired qualification

When any of the verified certifications is about to expire (2 months in advance) the service owner will receive (through email) a notification and can upload the new certification on the marketplace.

Image not found or type unknown



The certification can be renewed at any time, uploading a new VC validated by the DOME Trust Service Provider. If the certification is not re-newed by uploading a new VC the compliance profile will be automatically updated in the DOME platform. The service owner will get a notification about the new compliance level achieved by the service and this information will be updated in the Compliance Profile.

How to qualify a product (User Guide)

/Under construction/

The qualification process is being updated to the new DOME Compliance policy, please contact **dome-certification@listas.tecnalia.com**