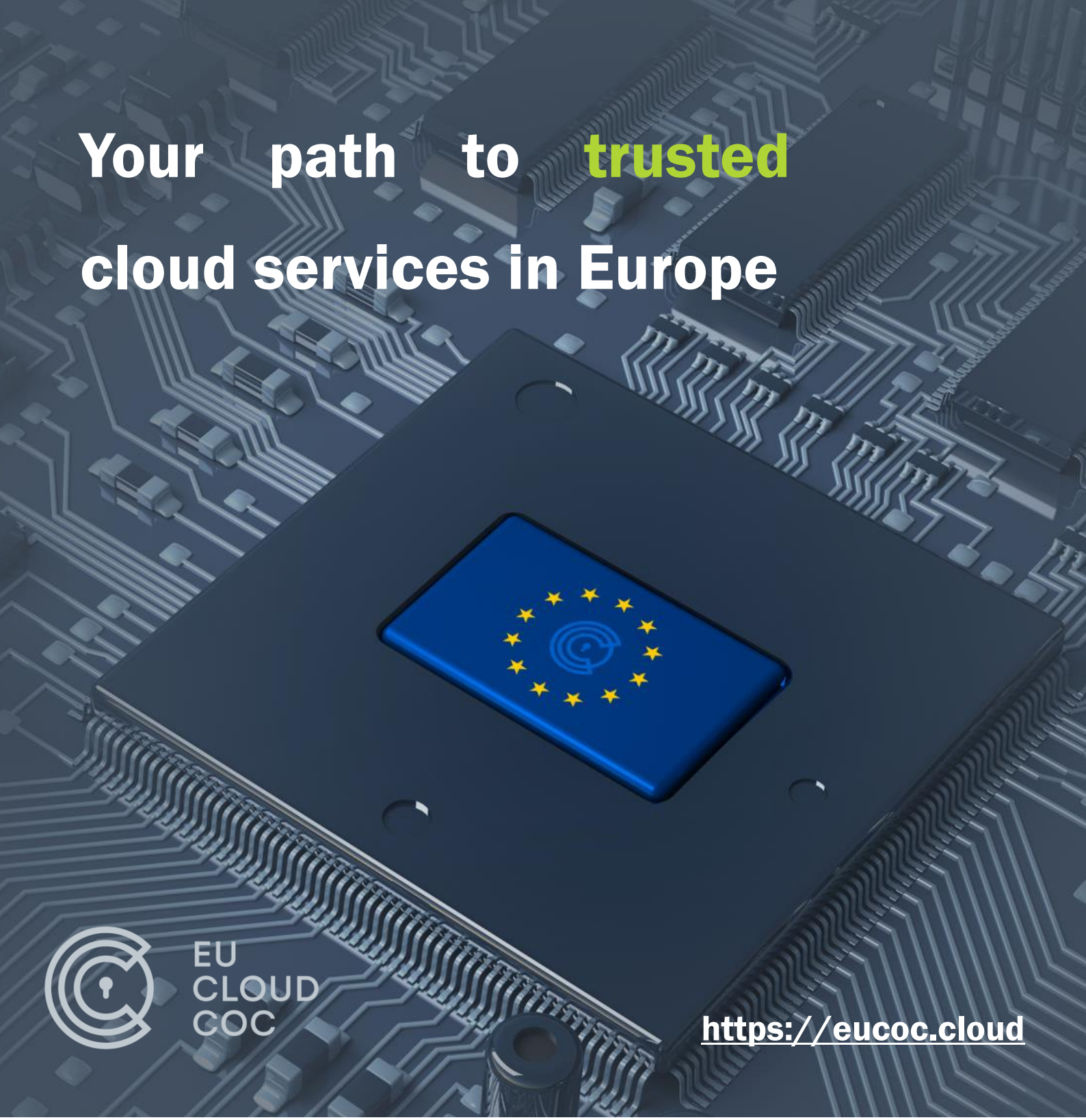

Level 3 Compliance

Guidelines and Requirements

January 2023

1 Changelog

Version	Time of Edit	applied changes
v.1.0	November 2022	• Beta Version
v.1.1	January 2023	• Original publication

1 Introduction

The EU Cloud Code of Conduct ("Code")[1] provides for three levels of compliance[2]. The level of compliance relates to the evidence submitted by the Cloud Service Provider ("CSP") to the accredited Monitoring Body ("Monitoring Body"), i.e., SCOPE Europe[3].

Level 1

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

Level 2

Compliance with the Code is **partially** supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which are based upon internationally recognised standards procedures.

Level 3

Compliance with the Code is **fully** supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which are based upon internationally recognized standards.

---

[1] https://eucoc.cloud; https://eucoc.cloud/get-the-code
[2] https://eucoc.cloud/en/public-register/levels-of-compliance
[3] https://scope-europe.eu

2 Scope and Intent

This Guidance provides general information, as well as recommendations, on the process and requirements to reach Level 3 Compliance to the Code. While some information will be relevant for CSPs, a significant share of information and recommendations address third party assessors ("Assessors") which will draft third party assessment reports to be submitted for the verification of a Level 3 Compliance by the Monitoring Body.

The purpose of this Guidance is to ensure a better understanding of the requirements for a Level 3 Compliance verification by the CSP and Assessors.

3 Mandatory Requirements for CSPs

For a Level 3 Compliance assessment, CSP's Declaration of Adherence shall be **fully supported by reports**, based upon internationally recognised standards. Reports may be in the form of third-party certificates, audits and individual reports (e.g., ISAE-3000 reports). CSP shall ensure that the reports submitted provide sufficient and assessable information and details on the actual measures implemented by the CSP with regard to the Cloud Service declared adherent.

Several reports may be submitted to the Monitoring Body, provided they cover **100% of the controls** of the Code ("Controls). This can be a combination of several reports and certifications. E.g., Section 6 of the Code, which relates to IT-Security, is closely aligned to ISO 27001. Consequently, compliance with Section 6 can be broadly supported with a current ISO 27001 certificate. Where the periods of reports will not perfectly match expected verification period under the Code, the CSP shall provide a confirmation that the CSP intends to renew any such reports.

Nonetheless, for the time being, the Code addresses a significant number of Controls that are not, yet, covered by any other internationally recognized standard. In other words, to reach Level 3 Compliance, CSPs are required to provide at least one individual report.

It is likely that such an individual report will have to cover Section 5 of the Code, as well as Controls 6.1.A, 6.1.B, 6.2.H, 6.2.I and 6.2.P.

Any information, including reports, submitted to the Monitoring Body should be in **English**.

4 Requirements for Assessors and/or Individual Reports

4.1 Identify the overarching methodology applied

All individual reports should specify the basis of the opinion of the Assessor, i.e., which **international standards** the individual reports are based upon, such as ISAE-3000. Where the assessment was performed retrospectively, the Assessors shall include a confirmation by the CSP that the implementation as reflected by such retrospective report will also be applicable in the future.

4.2 Clearly Identify the scope of the report

Each report should **indicate an exhaustive list** of services in scope and the period covered.

4.3 Deterministic language should be used

Use of generic language is to be avoided. **The Assessor should rather indicate the reasons as to why compliance was concluded.** Each Control and each dimension of a Control should be addressed clearly and separately, and a specific explanation on each Control should be provided.

If a Control is not applicable, an **explanation and reasoning** have to be provided as to why that Control would not apply to that Cloud Service or Cloud Service family.

4.4 Means by which compliance was validated shall be identified

Assessors should indicate per Control, how the validation has been performed. This might indicate aspects such as Interview, Document Review, Sampling etc. Where samples will be taken, the report should indicate the extent of such sample and the related total of which the sample was taken.

4.5 Relevant Information shall be provided by the Assessor

Any mapping of the Code's Controls to CSP's internal controls shall either be performed by the Assessor or alternatively where it has been performed by the CSP, the Assessor shall confirm its accuracy.

5 Additional Supportive Information

5.1 Final Decision by the Monitoring Body

Any final decision with regards to whether the Cloud Service or Cloud Service family meets all the requirements of Level 3 Compliance is at the sole discretion of the Monitoring Body.

Reports must not undermine the role and function, and thus the independence and powers of the Monitoring Body, as provided under the General Data Protection Regulation ("GDPR"). The Monitoring

Body reserves the right to question reports submitted as part of the process and make its own decisions.

5.2 Level 3 Compliance only if requirements are met

If the Monitoring Body concludes, that there is a remaining gap at the time of conclusion by the Monitoring Body, the Monitoring Body shall not grant a Level 3 Compliance. In that case, the Monitoring Body may and will still conclude on any other Level of Compliance, if applicable.

5.3 Timelines

It must be noted that due to the requirement of individual reports, additional preparations by the CSP will be required. In other words, in addition to the time necessary to process the declaration of adherence by the Monitoring Body, Assessors will need their due time to draft their reports. Consequently, it should be expected that a Level 3 Compliance verification may easily take between 3 to 6 months.

5.4 Costs

Level 3 Compliance has no additional costs at the Monitoring Body. Nonetheless, the CSP will have costs associated with the third-party reports to be submitted.

5.5 Upgrades and Downgrades

The CSP may always decide to upgrade or downgrade its Level of Compliance. Declarations of Adherence must be renewed annually. With such renewal, a CSP once verified as Level 3 compliant, may decide to not submit a full coverage of reports anymore. In this case, and provided compliance is still applicable, the Monitoring Body will conclude on any other applicable Level of Compliance, and this would not require additional reporting from a CSP but would rather follow the same renewal procedure. If a CSP is downgrading, the downgrade will not require any additional reasons.

The same logic applies if a CSP decides to submit initially a full coverage of reports with its renewal. If the submitted reports meet the requirements of a Level 3 Compliance, this will be granted without additional costs.

If a CSP wishes to upgrade its Level of Compliance before the due date of the renewal of a Declaration of Adherence, the CSP may do so as well. In this case, the CSP will trigger an early renewal subject to the ordinary pricing scheme.

5.6 Suitable third-party Assessors

In the future, the Monitoring body may decide to implement specific mechanisms to ensure that each Assessor providing individual reports has special knowledge and consistent interpretation of the Code. For the time being, no such additional requirements are applicable.

Nonetheless, it is recommended to ensure that such Assessor has decent knowledge of the Code or will reach out to the Monitoring Body before completing its report. This will ensure that the Assessors' report can be processed by the Monitoring Body as best as possible.

In this context, it shall be noted that the Code also provides a status as Supporter, which may indicate a deep interest in the Code and subsequent understanding of its requirements.

The Monitoring Body will assess the situation and the quality of reports received by third parties. As to the extent necessary, and provided by the Code, there might be further requirements applicable to such third parties in future, be it receiving mandatory trainings, being listed at the Code's or Monitoring Body's website, etc.

About EU Cloud CoC

The EU Cloud Code of Conduct is an approved and fully legally operational Code of Conduct pursuant to Article 40 GDPR. Defining clear requirements for Cloud Service Providers to implement Article 28 GDPR, the Code covers all cloud service layers (IaaS, PaaS, SaaS), has its compliance overseen by an accredited monitoring body, and represents the vast majority of the European cloud industry market share.