European Cloud Service
Data Protection Certification

Concept of Modularity

- Version 0.99c -

Status: 05/04/2022

Related AUDITOR documents:

- certification object
- criteria catalogue
- concept of protection categories
- DIN SPEC 27557

Available online at: www.auditor-cert.eu

Recommended Citation:

Sunyaev, A., Roßnagel, A., Teigeler, H., Lins, S. & Maier-Reinhardt, N. (2022). AUDITOR Concept of Modularity – Version 0.99c. Online available: www.auditor-cert.eu

Contribution to the research project "European Cloud Service Data Protection Certification (AUDITOR)," which, based on a resolution adopted by the German Parliament), is sponsored by the Federal Ministry for Economic Affairs and Energy (FKZ 01MT17003A).

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

Authors

Ali Sunyaev[a], Alexander Roßnagel[b], Heiner Teigeler[a], Sebastian Lins[a], Natalie Maier-Reinhardt[b]

[a] Research group: Critical Information Infrastructures (cii) of the Institute of Applied Informatics and Formal Descriptive Methods (AIFB) at the Karlsruhe Institute of Technology
[b] Project group: Constitutionally Compatible Technology Design (provet) at the Research Centre for Information Technology Design (ITeG) at the University of Kassel

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES

UNIKASSEL VERSITÄT

provet

Table of contents

List of abbreviations and acronyms

Art.	Article
GDPR	EU General Data Protection Regulation (applicable as of 25.5.18)
DSK	German Data Protection Conference (Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder)
EDPB	European Data Protection Board
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
Para.	Paragraph
SaaS	Software as a Service

Note on the gender-neutral wording:

All references to persons in the AUDITOR Criteria Catalogue shall be considered to be gender-neutral. Therefore, for the purpose of better readability, no gender-specific wording is used, while the male grammatical form shall apply to all genders equally (e.g., any use of the title “data protection officer” in combination with male pronouns is a reference to the functional description as gender-neutral and without specifically referring to a person of the male gender).

A. AUDITOR concept of modularity

1. Introduction

A central element of the AUDITOR certification scheme is the AUDITOR concept of modularity, which describes the horizontal and vertical modularisation of data processing operations. The AUDITOR concept of modularity increases flexibility in certification. For example, it is possible to certify a cloud service in its entirety or only a single data processing operation of the cloud service. In addition, the modularity concept serves as a basis for the recognition of equivalent certifications within the framework of an AUDITOR certification.

2. Object of certification

The object of certification in the AUDITOR certification mechanism comprises operations of processing personal data in the context of cloud services. According to Art. 4 (2) GDPR, data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. This includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data. The AUDITOR mechanism considers the data processing operations that the cloud provider carries out as a processor as part of processing in accordance with Art. 28 GDPR. Furthermore, data processing operations are also considered that the cloud provider performs as the controller to enter into and perform the contract on the provision of the cloud service with the cloud user or to fulfil legal obligations.

When determining the object of certification, there are three components that cloud providers must consider as addressees of the AUDITOR certification mechanism: 1. personal data; 2. technical systems (infrastructure, hardware and software used to process the personal data) and 3. processes and procedures related to the processing operations. Thus, a data processing operation usually consists not only of technical and automated but also of non-technical organisational components, which are integrated into data protection concepts and data protection management systems. The entire data processing operation must comply with the requirements of the General Data Protection Regulation.

Data processing operations must have a self-contained procedural structure for the processing of personal data, within which the specific data protection risks of the respective cloud service can be taken into account in full. This means that interfaces of the cloud service to be certified with other services must also be taken into account, so as to identify data flows from which data protection risks may arise.

Further information about the AUDITOR certification object can be found in the supplementary document "AUDITOR Certification Object", which contains a detailed definition of the object from a legal and technical point of view.

B. Horizontal and vertical modular certification

Modular certification reflects the fact that data processing operations are often designed in a modular way. Thus, a cloud provider offering several cloud services can combine or simplify the certification based on the interrelationships between them. Modularisation describes a process in which a cloud service and the corresponding data processing operations are divided into individual modules. Thus, it is possible for a cloud service to be fully certified by certifying all relevant data processing operations together. The cloud service then corresponds to a module. By contrast, it is also possible to certify only a single data processing operation of the cloud service. In this case, the data processing operation is to be understood as a single module. Modules that have already been certified can then be recognised in future certification processes (see Section C), so that the effort and costs associated with future certifications are reduced. Despite modularisation, it must be ensured that the modular data processing operations have a coherent and closed procedural structure for the processing of personal data and that no critical processing operations are excluded.

Modularisation of certification can take place on a horizontal as well as a vertical level. This distinction is shown in simplified form in Figure 1 and explained in the following sub-sections using the examples described there. In the figure, the three basic service models of cloud computing, i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), form the so-called service levels ('cloud stack').

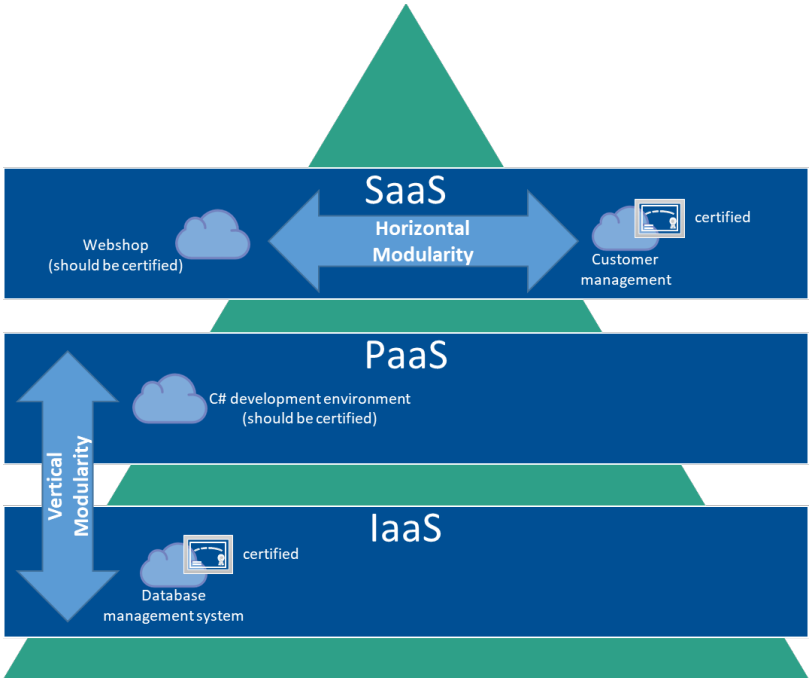

Figure 1. Examples of horizontal and vertical modularity

1. Horizontal modularisation of data processing operations

Horizontal modularisation describes the division of data processing operations or cloud services within a service layer of the cloud stack. If, for example, the customer management module (i.e. all data processing operations relevant in that context) has already been audited and certified, the module can be used for other connected cloud services. Thus, when certifying a cloud-based webshop (as an independent module), the existing customer management certificate can be recognised. The cloud provider benefits from horizontal modularisation if the cloud services overlap on one level (at the SaaS level, for example) or use identical data processing operations.

2. Vertical modularisation of data processing operations

A modular structure can also be identified in terms of composition across the different layers of the cloud stack. Vertical modularisation describes the division of data processing operations or cloud services across different service layers of the cloud stack. Vertical modularisation means that data processing operations that have already been certified can be recognised if a cloud service that requires certification at another level uses them. Similar to horizontal modularisation, this is only possible if two cloud services act together or are connected. The cloud provider benefits from the fact that the cloud services it offers often use data processing operations at lower levels of the cloud stack, for example identical systems, hardware or buildings. As shown in Figure 1, this vertical modularisation can occur, for example, between the PaaS and IaaS layers. If the database management system module of the IaaS has already been certified, this can be recognised in certification of another PaaS cloud service. In the example shown above, the cloud service to be certified, a C# development environment, would use the database management system that has already been certified and thus benefit from the existing certificate.

C. Recognition of existing certificates

1. Requirements and procedure for recognition

Recognition of existing certificates is mainly regulated by the supplementary requirements of the German Data Protection Conference (DSK) for accreditation according to Art. 43 (3) GDPR and the requirements of ISO/IEC 17065. AUDITOR certification basically follows these requirements.

Therefore, there are only three ways in which another certificate can be recognised as a partial evaluation within the certification process (see DSK para. 7.4, ISO/IEC 17065:2012 para. 6.2.2.4):

(1) The certificate has been issued by an accredited certification body (e.g. an ISO/IEC 27001 certificate by an accredited certification body);
(2) The certificate has been issued by a body that has undergone an assessment among peers (according to ISO/IEC 17040:2005);
(3) The certificate has been issued by a government certification body on a legal basis (e.g. the Cyber Security Act).

If the cloud provider seeks recognition of existing certificates for components of its data processing operation, the certification body must immediately check whether and to what extent recognition can take place on the basis of the guidelines defined in the conformity assessment scheme. As a matter of principle, the equivalence of the certificate must always be checked (see C.2). The requirements and necessary checks are detailed below.

Requirements for recognition

- The certificate
  (1) confirms successful **data protection certification in accordance with Art. 42 GDPR**, or
  (2) confirms another successfully completed certification process of an **accredited certification body**, or
  (3) has been issued by a body that has undergone **peer assessment** (according to ISO/IEC 17040:2005), or
  (4) has been issued by a **state certification body on a statutory basis**.
- The **certification body** that has carried out the audit according to the certification criteria and issued the certificate must
  (1) be accredited according to ISO/IEC 17065 in conjunction with the additional requirements of the DSK for accreditation according to Art. 43 (3) GDPR, or
  (2) be accredited based on the requirements of the certificate issued (e.g. ISO/IEC 17021, 17025, 17065).

- A complete certification report (including a report on determination activities and their findings) is necessary for assessment of recognition. A simple certificate or similar marks of conformity are not sufficient.
- The criteria to be recognised must meet the level of protection for the AUDITOR certification process (in particular the protection category and restorability class).
- The data processing operation to be certified must be part of the scope of the existing certificate (e.g. data processing operation is part of the ISMS certified according to ISO/IEC 27001).
- The certification process underlying the certificate must be completed at the time of application (see DSK point 7.4).

Examples of certificates that may be recognised

(1) European Privacy Seal (EuroPriSe) (as soon as it is approved in accordance with Art. 42 GDPR)
(2) ePrivacyseal EU (as soon as it is approved in accordance with Art. 42 GDPR)
(3) ISO/IEC 27001
(4) ISO/IEC 9001

Supplementary notes:

The AUDITOR Criteria Catalogue contains per criterion individual implementation guidance. “Implementation guidance” serve as guidance using typical examples for understanding and implementing the criteria; however, they are not binding. Implementation guidances are also not conclusive but they describe central implementations of the criteria. The implementation guidance are based on existing industry standards, norms and best practices as appropri-ate. For example, with regard to the criteria under no. 2 for the assurance of data security, in particular, it is referred to ISO/IEC 27002 and BSI C5. Reference to these standards and (industry-specific) best practices, however, do not give any indication of possible recogni-tion within the framework of AUDITOR certification. In particular, the possibilities of recogni-tion described in (2) apply. As a consequence, a BSI C5 certificate will not be able to

be recognised in the AUDITOR framework even though it is referred to in the implementation guidance.

Implications in the event of recognition

- If the certification body recognises certificates for components of data processing operations, current compliance with the criteria (of the submitted certificate) must be verified at least on the basis of sampling and the existing certificate must be assessed.
- The validity period of the AUDITOR certification is restricted to the expiry date of the shortest current, recognised certificate (see DSK point 7.4). In the case of recertification of the recognised certificate, the expiry date of the AUDITOR certification is extended to the term of the recognised certificate, but up to a maximum of the standard term of the AUDITOR certification of 3 years or, if there are other recognised third-party certificates, to the shortest term. If no recertification of the recognised certificate is carried out, the area originally covered must be audited again as a minimum in order to maintain the validity of the AUDITOR certification.

Tasks of the cloud providers

- Notification of the certification body that the intention is to have existing certificates recognised (see DSK point 7.4).
- Submission of the available certification documents to the certification body. These include among others:
  (1) certificate or similar marks of conformities;
  (2) complete certification report, including a report on determination activities and their findings. If this is not possible (e.g. no disclosure of the documents for legal or contractual reasons), the cloud provider must provide sufficient information to enable an assessment of the certificate (see DSK para. 7.4, EDPB Annex 1 para. 7.4). This includes, in particular, a clear and detailed description of the scope of certification;
  (3) criteria catalogue for the certification;
  (4) detailed description of the object of certification, including description of the interfaces with or transitions to other systems and organisations (e.g. ISO/IEC 27001 Statement of Applicability, SoA).

- Notification of the certification body with sufficient time in advance if a recognised certificate is about to lose its validity as scheduled (i.e. on expiry of the validity period) or not as scheduled (i.e. before the end of the regular validity period of the certification body) and what actions the cloud provider wants to take (e.g. recertification). If the cloud provider does not seek recertification of the recognised certificate, the area originally covered must be audited again as a minimum in order to maintain the validity of the AUDITOR certification.

Tasks of the certification body

- Critical evaluation of existing certificates and its related certification, and documentation of the extent to which it can be recognised. Availability of a complete certification report (including a report about determination activities and their findings) or information that enables an assessment of the certification activities and results (see DSK para. 7.4, EDPB Annex 1 para. 7.4) is necessary for assessment of recognition.
- Where the certification body recognises certificates for components of data processing operations, a complete assessment of the component of the data processing operation named in the certificate is not required. However, the certification body is still obliged to check current compliance with the criteria (of the submitted certificate) at least on the basis of sampling and to evaluate existing certificates.
- Assessment of the interaction of the recognised component of the data processing operation with other components, in particular the interfaces relevant to that interaction, is also required.
- If irregularities arise within the scope of AUDITOR certification with regard to recognised certificates (e.g. suspicion of non-conformities), the determination activities must be expanded within the scope of the ongoing certification process and, if necessary, extended to the entire object that has already been certified (see DSK para. 7.4, EDPB Annex 1 para. 7.4).
- Recognition must be justified and adequately documented, especially with regard to the protection category and restorability class. In particular, it must be documented how and to what extent recognition is granted and what concrete effects it has on the remaining scope of determination and the determination activities (see DSK point 7.4).

- The expiry date of the recognised certificates must be noted and kept for the decision. If existing certificates of the cloud provider are recognised, the validity period of the AUDITOR certification is restricted to the expiry date of the shortest current, recognised certificate (see DSK point 7.4). The certification body notes the validity period of the recognised certificates. The ongoing validity of the recognised certificates is checked by the certification body as part of the surveillance activities as a minimum. If the cloud provider informs the certification body that recertification of the recognised certificate has been carried out, the expiry period of the AUDITOR certification is extended to the validity period of the recognised certificate, but up to a maximum of the standard AUDITOR certification validity period of 3 years or, if there are other recognised third-party certificates, to the shortest validity period. If no recertification is carried out, the area originally covered area must be re-audited by the certification body as a minimum in order to maintain the AUDITOR certification.

2. Equivalence of existing certificates

A requirement for the recognition of certificates from other certification bodies is that the audit by the certification body whose certificate requires recognition is equivalent to its own audit. As a rule, equivalence exists in the case of certificates issued by an accredited certification body, and thus in particular in the case of approved data protection certificates in accordance with Art. 42/43 GDPR.

Both material and procedural equivalence of conformity assessment results must be ensured to maintain the same level of confidence in conformity (see DSK para. 7.4, ISO/IEC 17000:2004 para. 7.4). Material equivalence exists if the existing certificate is based on certification criteria that are equivalent to or exceed those of the AUDITOR criteria catalogue with regard to the level of protection. The certification body determines in particular the protection category and restorability class in which the certificate is recognised. Procedural equivalence exists if the other certificate was issued on the basis of an accredited certification process that offers a comparable guarantee for proper determination and certification activities.

In the case of a combination of certificates from different certification bodies, questions arise regarding responsibility and liability that require further discussion. However, this does not change the fact that it is possible to rely on certificates of other certification bodies, provided that the audit carried out in connection with them is equivalent to the certification body's own audit and meets the requirements pursuant to Art. 43 (3) GDPR and the requirements of the DSK. The essential basis of a system of modular certification is thus that there is transparency and legal certainty with regard to the audit requirements and the equivalence of audits.

D. References

DSK	Requirements for Accreditation (in German: Anforderungen zur Akkreditierung gemäß Art. 43 Para. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065. Version 1.2 (21.01.2020). Vorläufige Fassung)
EDPB Annex 1	EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1. Version 3.0, as of 04.06.2019
ISO/IEC 17065:2012	Conformity assessment — Requirements for bodies certifying products, processes and services. Published: 2012