European Cloud Service
Data Protection Certification

AUDITOR Conformity Assessment Scheme

- Version 0.99d -

Status: 04/05/2022

Related AUDITOR publications:

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

Available online: 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], Sebastian Lins [a], Natalie Maier-Reinhardt [b], Johannes Müller [b], Heiner Teigeler [a]

[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

UNIKASSEL VERSITÄT

provet

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES

Table of contents

List of abbreviations and acronyms

Art.	Article
AUDITOR	European Cloud Service Data Protection Certification (name of the research project)
BDSG	German Federal Data Protection Act (applicable as of 25.05.18)
DAkkS	German Accreditation Body (Deutsche Akkreditierungsstelle GmbH)
GDPR	EU General Data Protection Regulation (applicable as of 25.05.18)
DSK	Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder (Datenschutzkonferenz)
IaaS	Infrastructure as a Service
Lit.	Litera (letter)
No.	Number
PaaS	Platform as a Service
SaaS	Software as a Service
Subs.	Subsection
TCDP	Trusted Cloud Data Protection Profile
TOM	Technical and organisational measures
UrhG	German Copyright Act (Urheberrechtsgesetz)

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).

1 Introduction

1.1 Function and objectives of the AUDITOR conformity assessment scheme

The AUDITOR certification provides evidence of the compliance of cloud providers' data processing operations with the requirements of the EU General Data Protection Regulation (GDPR). Pursuant to Art. 43 (1) sentence 1 GDPR, certification bodies may issue certifications alongside data protection supervisory authorities. However, a certification body may only commence its activities if it has been accredited by the German Accreditation Body (Deutsche Akkreditierungsstelle GmbH; DAkkS) in cooperation with the responsible data protection supervisory authority. The prerequisite for accreditation is compliance with the requirements pursuant to Art. 43 (2) GDPR and the supplementary requirements of the German Data Protection Conference (DSK) for accreditation pursuant to Art. 43 (3) GDPR in conjunction with ISO/IEC 17065.

Crucial for accreditation is a conformity assessment scheme, which must be developed for each certification individually. The conformity assessment scheme describes the specific requirements, rules determination activities that must be used for the conformity assessment of data processing operations in order to be able to make the statement associated with the certification in a scientifically traceable and systematic manner (see DAkkS 71 SD 0 016). The present *'AUDITOR Conformity Assessment Scheme'* therefore describes the principles to be fulfilled by the certification body and essentially comprises requirements for the certification body and the certification process. The AUDITOR conformity assessment scheme is managed and further developed by the Competence Network Trusted Cloud e.V. as the scheme owner. It is made available to interested certification bodies on non-discriminatory terms to ensure a broad application of the certification process.

1.2 TCDP development pursuant to the General Data Protection Regulation

The certification pursuant to the old German Federal Data Protection Act was examined in the pilot project "Data Protection Certification for Cloud Services" by the Trusted Cloud Data Protection Profile (TCDP), which was finalised in September 2016. Since not all relevant international standards, newly developed relevant sets of criteria – e.g. ISO 27701 – and, in particular, not the requirements of the General Data Protection Regulation could be taken into account when developing the certification criteria according to TCDP, the TCDP criteria must be adapted to the new regulations as of the application of the General Data Protection Regulation on 25 May 2018. This is done in the AUDITOR Criteria Catalogue. The AUDITOR Criteria Catalogue focuses on all relevant regulations for the data protection certification of cloud services in the General Data Protection Regulation and specifies them to create testable criteria.

The pilot project has already developed rules and procedures for certification under the TCDP. However, this certification process was not accredited. TCDP's existing rules and procedures were taken into account in the course of the development of the AUDITOR conformity assessment program. An adaptation of the TCDP rules and procedures is necessary with regard to the requirements according to Art. 43 (2) GDPR and the supplementary requirements of the DSK for accreditation according to Art. 43 (3) GDPR in conjunction with ISO/IEC 17065, which will be done in the course of this conformity assessment scheme.

1.3 Structure and contents of the conformity assessment scheme

The AUDITOR conformity assessment scheme is divided into four essential sections. Section 2 sets out the purpose of the conformity assessment scheme and defines key terms. Section 3 regulates the principles for carrying out certification activities in order to establish confidence in the certification activities and results. Section 4 sets out requirements for the certification body, including, for example, requirements regarding the structure and resources of the certification body. Section 5 describes requirements for the certification process, divided into the process phases of selection, determination, review, decision, attestation and surveillance.

When specifying a conformity assessment scheme, it is essential to define how the individual criteria need to be evaluated to ensure that different evaluators arrive at the same conformity assessment result. The supplementary document '*AUDITOR Determination Activities'* therefore specifies how each criterion should be verified during the determination activities.

2 Basics

2.1 The AUDITOR conformity assessment scheme

§ 2.1.1 Designation of the conformity assessment scheme

(1) The name of this scheme is: AUDITOR conformity assessment scheme.
(2) The name of the certification is “GDPR CC”.

§ 2.1.2 Purpose of the conformity assessment scheme

(1) The aim of AUDITOR certification is to create confidence in the data processing of cloud services when processing personal data.
(2) The AUDITOR certification provides proof of compliance of cloud providers' data processing operations with the requirements of the General Data Protection Regulation.
(3) This conformity assessment scheme sets out requirements for the certification body and certification process to ensure that the AUDITOR certification process is operated competently, consistently and impartially by certification bodies.
(4) This conformity assessment scheme is also intended to ensure that the requirements of Art. 43 (2) GDPR and the supplementary requirements of the DSK for accreditation according to Art. 43 (3) GDPR in conjunction with ISO/IEC 17065 are met.

§ 2.1.3 Conformity assessment type

(1) This conformity assessment scheme comes under the conformity assessment type "certification" as defined in ISO/IEC 17065:2012.
(2) This scheme comes under scheme type 6 as defined in ISO/IEC 17067:2013 subs. 5.3.8.

§ 2.1.4 Scheme owner

(1) The scheme owner is a person or organisation responsible for the development and maintenance of this conformity assessment scheme (see ISO/IEC 17065:2012 subs. 3.11). The scheme owner arranges and monitors certification bodies’ compliance with the certification requirements through a legally binding agreement with accredited certification bodies (see DAkkS 71 SD 0 016).
(2) The scheme owner of this conformity assessment scheme is the Competence Centre Trusted Cloud e.V. An advisory board has been set up at the Competence Centre Trusted Cloud e.V. to implement, manage and steer this scheme (see ISO/IEC 17067:2013 subs. 6.3.5). The advisory board is the decision-making body in relation to

(a) amendments/additions to the AUDITOR Criteria Catalogue,
(b) amendments to the AUDITOR conformity assessment scheme,
(c) issues of internationalisation and standardisation
(d) cooperative ventures

(3) It has an advisory function in all questions relating to the marketing approach and licensing of the certification. The advisory board comprises the following representatives:

(a) 2 representatives of the Karlsruhe Institute of Technology (planned: Prof. Sunyaev; Mr. Lins)
(b) 2 representatives of the University of Kassel (planned: Prof. Roßnagel, Prof. Hornung)
(c) 2 representatives of the Federal Ministry for Economic Affairs and Energy (planned: Dr. Tettenborn; Dr. Werner)
(d) 1 representative of the Federal Ministry of the Interior (to be appointed)
(e) 1 representative of the competence network Trusted Cloud e.V. (planned: Mr. Niessen)

Other experts in the fields of business, politics and science may be consulted; this includes the members of the current steering committee and expert advisory board of the AUDITOR research project (including Bitkom, Stiftung Datenschutz, BfDI).
(4) The scheme owner takes full responsibility for the objectives, content, and completeness of this scheme (see ISO/IEC 17067:2013 subs. 6.3.4).
(5) The scheme owner maintains this scheme and provides guidance to certification bodies as required (see ISO/IEC 17067:2013 subs. 6.3.5). The following activities are carried out for this purpose:

(a) implementation of changes to the certification criteria (see ISO/IEC 17067:2013 subs. 6.6.2);
(b) leading the standardisation activities of the certification criteria (e.g. transfer to DIN, CEN/CENELEC or ISO standard);
(c) implementation of changes to this conformity assessment scheme;
(d) monitoring of
    (i) changes in the legal framework resulting from amendments to laws, the adoption of delegated acts by the European Commission, decisions of the European Data Protection Board and court rulings;
    (ii) advancements in the state of the art of technology;
    (iii) changes to requirements of data protection supervisory authorities and the European Data Protection Board (EDPB) for criteria catalogues and certification process;
    (iv) legal acts and other requirements of the EDPB or data protection supervisory authorities.
(e) informing the accredited certification bodies of relevant or significant changes;
(f) coordination of collaboration with stakeholders to maintain and further develop the scheme and certification criteria;
(g) implementation and coordination of activities for the internationalisation of certification, e.g. submission for European Data Protection Seal to the EDPB;
(h) consultative activities on all issues relating to market approach;
(i) exchange of information and coordination with DAkkS, DSK, German task group “certification” of data protection authorities (“AK Zertifizierung”), and national data protection supervisory authorities.

(6) The scheme owner assesses the risks/liabilities arising from its activities and manages them accordingly (see ISO/IEC 17067:2013 subs. 6.3.10).
(7) The scheme owner ensures that information about this scheme is made available to the public to ensure transparency, understanding and acceptance (see ISO/IEC 17067:2013 subs. 6.4.5). To this end, the following measures are implemented:

(a) publication of the certification criteria in the AUDITOR Criteria Catalogue with free access for all stakeholders on the Internet;
(b) sharing of this scheme with cloud providers, data protection supervisory authorities, certification bodies and other stakeholders as required by submitting the scheme electronically.

§ 2.1.5 Scope of application

(1) This conformity assessment scheme sets out certification requirements for the competence, consistent operation and impartiality of certification bodies for data protection certification of data processing operations in cloud services in accordance with the requirements of the General Data Protection Regulation.
(2) AUDITOR certification is open to all private cloud providers who act as processors within the meaning of Art. 4 No. 8 GDPR and wish to demonstrate the compliance of their data processing operations with the General Data Protection Regulation.
(3) The certification criteria are defined in the relevant version of the AUDITOR Criteria Catalogue.
(4) This conformity assessment scheme is made available to interested certification bodies on non-discriminatory terms to enable accreditation under this scheme and to ensure wide use of the certification process.

§ 2.1.6 Changes to this conformity assessment scheme

(1) Changes to this conformity assessment scheme are made by the scheme owner.
(2) The scheme owner undertakes to notify the accredited certification bodies, cloud providers certified under this scheme, the data protection supervisory authority, the DAkkS and other stakeholders, if required, of future changes to the scheme in a timely manner via suitable communication channels. Once the changes have been approved (usually by the DAkkS and the relevant data protection supervisory authority), the accredited certification bodies and certified cloud providers must also be informed in a timely manner.

§ 2.1.7 Development history

(1) This conformity assessment scheme was developed as part of the AUDITOR research project by the Critical Information Infrastructures research group, led by Prof. Dr. Ali Sunyaev and staff members Sebastian Lins and Heiner Teigeler at the Karlsruhe Institute of Technology, and the Project Group for Constitutionally Compatible Technology Design (provet), led by Prof. Dr. Alexander Roßnagel and staff member Dr. Natalie Maier-Reinhardt at the University of Kassel.

(2) Other parties participated in the revision and shaping of this scheme, including:

(a) CLOUD&HEAT Technologies GmbH;
(b) datenschutz cert GmbH;
(c) DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN e.V.;
(d) ecsec GmbH;
(e) EuroCloud Deutschland_eco e.V., eco - Verband der Internetwirtschaft e.V.;
(f) Competence Network Trusted Cloud e.V.;
(g) and other associated partners of the project.

2.2 Terminology

§ 2.2.1 Certification body

(1) Certification according to AUDITOR is performed by an independent and competent certification body, which acts as a third party in the sense of a conformity assessment body (see ISO/IEC 17000:2004 subs. 2.5, DSK subs. 4.2.1).

(2) The certification body must be a legally responsible organisation or a distinct part of a legally responsible organisation. According to Article R 17 (3) sentence 1 of Decision No. 768/2008/EC, a certification body must be an independent third party that has no connection with the institution it assesses (see DSK subs. 4.2.1).

(3) The certification body performs its activities in a non-discriminatory, confidential and impartial manner.

(4) Certification bodies must be accredited in accordance with ISO/IEC 17065 in conjunction with the supplementary requirements for accreditation pursuant to Art. 43 (3) GDPR and this scheme in order to demonstrate compliance with the certification requirements, in particular compliance with the basic certification principles.

(5) The certification body has a contractual relationship with the cloud provider to be certified and, if applicable, with outsourced evaluators.

§ 2.2.2 Evaluation

(1) Evaluation refers to the conformity assessment functions of selection and determination (see ISO/IEC 17065:2012 subs. 3.3).

§ 2.2.3 Evaluators

(1) Evaluators for the purposes of this scheme are natural persons who are members of the certification body and who perform selection and/or determination activities under this scheme.

(2) A certification body may also appoint an outsourced, independent and competent conformity assessment body or (individual) external evaluators to perform the selection and/or determination activities according to ISO/IEC 17065:2012 subs. 6.2.2 (see § 4.2.5). Personnel of these conformity assessment bodies and external evaluators are referred to as outsourced evaluators. They perform their activities in a non-discriminatory, confidential and impartial manner.

(3) Conformity assessment bodies and outsourced evaluators have a contractual relationship with the certification body. A contractual relationship must not exist with the cloud provider to be certified (see § 4.2.5).

§ 2.2.4 Decision-makers

(1) Decision-makers for the purposes of this scheme are natural persons who are members of the certification body and who perform the review and/or make the decision on certification and/or subsequently the attestation of certification.

§ 2.2.5 Accreditation body

(1) An accreditation body is an authoritative body that performs accreditations (see ISO/IEC 17000:2004 subs. 2.6).

(2) An accreditation is a confirmation by a third party that formally states that a conformity assessment body (here certification body) has the competence to carry out specific conformity assessment tasks (here certification) (see ISO/IEC 17000:2004 subs. 5.6).
(3) In Germany, the DAkkS is solely responsible for performing accreditations.

§ 2.2.6 Object of certification

(1) The object of certification (within the meaning of subs. A.2.2 ISO/IEC 17000:2004, Annex A) is data processing operations for personal data within the meaning of Art. 4 No. 1 GDPR which are provided in cloud services or with the help of (also several) cloud services.
(2) The supplementary document *'AUDITOR Certification Object'* for this scheme contains a detailed derivation and description of the certification object. Certification bodies and (outsourced) evaluators must familiarise themselves with this document.

§ 2.2.7 Cloud services

(1) Cloud services for the purposes of this conformity assessment scheme are cloud services as defined by the National Institute of Standards and Technology (NIST) (2011).
(2) Cloud services provide flexible and on-demand access to a shared pool of configurable IT resources that can be accessed anytime, anywhere via the internet or a network.
(3) The features that characterise cloud services are on-demand access, a network connection, the possibility of resource pooling, high scalability and usage-based payment:

(a) On-demand self-service. On-demand self-service enables cloud users to customise the performance parameters of utilised cloud services independently and almost immediately. Notably, this can be done automatically and without human interaction with the respective cloud providers.
(b) Broad network access. Cloud services are provided via a broadband network, usually over the internet.
(c) Resource pooling. The resources made available by the cloud provider are used simultaneously by multiple cloud users through a multi-client architecture. In the process, the physical and virtual resources are allocated dynamically to different cloud users as needed.
(d) Rapid elasticity. The resources provided can be increased or shared flexibly and quickly, in some cases fully automatically, in order to match the resources to current needs.
(e) Measured service. In order to make cloud services measurable and transparent, cloud services control and optimise resource usage based on service-dependent measures, such as storage space, computing power or bandwidth. As a result, usage-based billing (referred to as 'pay-per-use') can be offered and implemented. Furthermore, resource usage is monitored, controlled, logged and communicated, in order to create transparency with regard to usage for both the cloud user and the cloud provider.

(4) In the context of this conformity assessment scheme, a distinction is made between the three basic service models of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In addition, a large number of other service models can be found in practice and in the literature, e.g. Database as a Service or Security as a Service. However, these specific service models can generally be assigned to the basic models of IaaS, PaaS, and SaaS.

(a) SaaS. The cloud user can access the software applications offered by means of various devices either via a thin-client interface (e.g. a web browser) or via application programming interfaces.
(b) PaaS. The cloud user can install and operate self-developed or purchased applications on the cloud infrastructure of the cloud provider. Operating systems, databases, programming environments, programme libraries or other services and tools supported by the cloud provider are used for this purpose.
(c) IaaS. The cloud user has access to (virtualised) hardware resources of the cloud provider, including computing power, storage capacities or networks. These can be used to install and operate any software, such as operating systems or applications.

(5) Cloud services can also be a part of other cloud services, so that in practice nested value chains or networks of cloud services increasingly occur. The responsibilities of the cloud provider and the dependencies on and interfaces with other cloud services must therefore be clearly named and differentiated in the certification process.

(6) Cloud services are services within the meaning of ISO/IEC 17065:2012.
(7) The supplementary document *'AUDITOR Certification Object'* contains a detailed description of cloud services as a certification object.

§ 2.2.8 Data processing operations in cloud services

(1) According to Art. 4 no. 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.
(2) A data processing operation can contain both technical and automated procedural steps and non-technical and thus also organisational (e.g. manual or personnel) steps, which can also include data protection concepts and management systems.
(3) The entire processing operation must comply with the requirements of the General Data Protection Regulation.
(4) Data processing operations must have a closed structure for the processing of personal data within which the specific data protection risks of the respective cloud service can be fully captured. This means that interfaces of the cloud service to be certified with other services must also be considered in order to identify data flows from which data protection risks may arise.
(5) The suitability of a data processing operation for AUDITOR certification is checked during the selection activities (see 5.1).
(6) The supplementary document *'AUDITOR Certification Object'* contains a detailed description of data processing operations in cloud services as a certification object.

§ 2.2.9 Cloud provider

(1) Cloud providers are legal entities that operate cloud services.
(2) Cloud providers constitute the clients of the certification body.
(3) Cloud providers are responsible for ensuring that the certification criteria are met (see ISO/IEC 17065:2012 subs. 3.1).

§ 2.2.10 Sub-processor

(1) A cloud provider may, as part of its data processing operations, involve other sub-processors who provide external resources and services to perform the data processing operations.
(2) Sub-processors are legal entities that operate products or services relevant to the data processing operations to be certified.
(3) A sub-processor is independent of the cloud provider.
(4) If the processing operations of a cloud service to be certified are based on non-proprietary platforms or infrastructures or if the cloud provider uses other sub-processors, the certification can only relate to those data processing operations which are within the area of responsibility of the respective cloud provider. However, the cloud provider must ensure that any third-party platforms, infrastructures and sub-processors used also comply with the data protection regulations relevant to them and only use such for the provision of its service.

§ 2.2.11 Cloud users

(1) For the purposes of this scheme, a cloud user is any natural or legal person who, as a controller pursuant to Art. 4 No. 7 GDPR, carries out processing operations on personal data and decides, alone or jointly with others, on the purposes and means of such processing operations and decides to outsource such processing operations to a cloud provider..
(2) Cloud users thus constitute the customers of the cloud provider.

§ 2.2.12 Data protection supervisory authority

(1) A data protection supervisory authority is an independent governmental body established by a Member State pursuant to Art. 51 GDPR (see Art. 4 (21) GDPR).
(2) A competent data protection supervisory authority is a data protection supervisory authority which is concerned with the processing of personal data because

(a) the cloud user as controller or the cloud provider as processor is established in the territory of the Member State of that data protection supervisory authority;
(b) the processing has or is likely to have a significant impact on data subjects residing in the Member State of that data protection supervisory authority;

(c) a complaint has been filed with this data protection supervisory authority (see Art. 4 (22) GDPR).

(3) As an accreditation body, the DAkkS accredits the certification bodies jointly with the competent data protection supervisory authority. The competent data protection supervisory authority grants the certification body the authority to act as such in an independent procedure on the basis of this joint accreditation (see DSK 'Foreword').

§ 2.2.13 European Data Protection Board

(1) The European Data Protection Board (EDPB) was established as a body of the European Union with its own legal personality and consists of the head of a data protection supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives (see Art. 68 (1) and (3) GDPR).

(2) The European Data Protection Board may approve the certification criteria so that this leads to a common certification, the European Data Protection Seal.

§ 2.2.14 Certification criteria

(1) Certification criteria are the normative requirements defined in the AUDITOR Criteria Catalogue that must be fulfilled by the cloud provider as a condition for establishing and maintaining certification.

(2) The approved criteria are published in electronic form by the scheme owner in accordance with Art. 42 (5) GDPR, stating the respective period of use (see DSK subs. 4.6, EDPB Annex 1 subs. 4.6).

§ 2.2.15 Certification requirements

(1) Requirements of the certification body and the certification process specified by this conformity assessment scheme.

§ 2.2.16 Protection categories

(1) The AUDITOR Criteria Catalogue differentiates certain criteria according to protection categories and defines different certification criteria for these that must be fulfilled. Protection categories are an important instrument in the AUDITOR certification because they can be used to express the individual protection requirements of data processing operations and their fulfilment by certified cloud services.

(2) When applying for certification, a cloud provider specifies the appropriate protection category for its cloud service.

(3) On the basis of its determination activities, the certification body establishes an assessment of the compliance of the data processing operations with the certification criteria of the AUDITOR Criteria Catalogue in relation to a specific protection category. However, the certification body does not assess the choice of a protection category. The protection category is determined and applied for solely by the cloud provider and the certification body adjusts the scope of its determination activities accordingly.

(4) The supplementary document *'AUDITOR Protection Category Concept'* contains a detailed description of the basic principles and forms of the protection categories. Certification bodies and (outsourced) evaluators must familiarise themselves with this document.

§ 2.2.17 Mark of conformity

(1) A mark of conformity is issued by a certification body to prove that a certification object conforms to specified certification criteria (see ISO/IEC 17030:2009 subs. 3.1).

(2) A certificate and a graphical quality seal are awarded as AUDITOR marks of conformity (see § 5.5.2, § 5.5.3, § 5.5.4).

§ 2.2.18 Interested parties

(1) Interested parties are companies, private persons, authorities, etc., who are interested in participating in the design of or involvement in the certification and/or who are aware of the certification and its mark of conformity on the market.

(2) Interested parties may in particular be:

(a) cloud users;
(b) customers of cloud users;
(c) data protection supervisory authorities;

(d) participants in the cloud market;
(e) other certification bodies.

3 Fundamental principles

The certification body undertakes to comply with the following fundamental principles for performing certification activities to ensure confidence in the AUDITOR certification process and the marks of conformity issued.

§ 3.1.1 Creating confidence

(1) The overall objective of certification is to create confidence among all stakeholders (see ISO/IEC 17065:2012 subs. A.1.1) that data processing operations in cloud services meet specified certification criteria. The value of a certification corresponds to the level of public confidence conveyed by impartial and competent certification bodies.

(2) The objectives of certification are to enable cloud providers to demonstrate to the market that their data processing operations comply with specified certification criteria through validation by an impartial third party (see ISO/IEC 17067:2013 subs. 4.2.1).

§ 3.1.2 Impartiality

(1) In order to build confidence in their activities and results, it is necessary for certification bodies and their personnel to be impartial and to be perceived as impartial by stakeholders (see ISO/IEC 17065:2012 subs. A.2.1).

(2) Impartiality describes the existence of independence and objectivity (see DSK subs. 4.2). Independence means that the certification body can act completely free of instructions and pressure and that its financial stability is ensured (see DSK ‘Chapter 5'). Objectivity means that conflicts of interest do not exist or have been resolved to ensure that such conflicts do not adversely impact certification activities.

(3) The certification body is responsible for the impartiality of its certification activities. It must not allow commercial, financial, or other pressures to compromise its impartiality.

(4) The certification body is responsible for ensuring that outsourced evaluators also perform their activities impartially, and continuously comply with the requirements for impartiality. In particular, there is an unacceptable risk to impartiality if there are contractual relationships between cloud providers requiring certification and outsourced evaluators who perform evaluation activities.

(5) Risks to impartiality may include bias, which may arise from (see ISO/IEC 17065:2012 subs. A.2.2):

- (a) self-interest (e.g. excessive dependence on a service contract or on fees, fear of losing the cloud provider or of becoming unemployed to an extent that adversely affects impartiality of certification activities);
- (b) self-review (e.g. performing certification activities where the certification body evaluates the results of other services it has already provided, such as consultancy services);
- (c) advocacy (e.g. when a certification body or its personnel acts in favour of or against a particular company which is also its client);
- (d) over-familiarity (e.g. risks attributable to a certification body or its personnel who are over-familiar or too trusting, instead of seeking evidence of conformity):
- (e) intimidation (e.g. the certification body or its personnel may be deterred from acting impartially by risks from, or fear of, a cloud provider or other party);
- (f) competition (e.g. between the cloud provider and a contracting person, or certification bodies on the market).

(6) In particular, a certification body’s personnel must not evaluate data processing operations or make certification decisions regarding data processing operations for which they have provided consulting in the last 24 months (see ISO/IEC 17065:2012 subs. 4.2.10).

(7) The source of revenue for the certification body is the payment for certification by the cloud provider. This poses a potential threat to impartiality. However, the certification body must ensure that the type and amount of payment does not influence the independence and objectivity of the certification activities.

§ 3.1.3 Competence

(1) In order to offer certifications that provide confidence, the competence of the personnel involved is essential and must be supported by the management system of the certification body (see ISO/IEC 17065:2012 subs. A.3).

(2) The certification body ensures that (outsourced) evaluators continuously demonstrate the necessary competence to perform (outsourced) activities.

§ 3.1.4 Confidentiality and openness

(1) The balance between certification requirements related to confidentiality and openness has an impact on the confidence of interested parties and their perception of the value of the certification.

(2) The certification body ensures that (outsourced) evaluators perform their activities confidentially.

(3) In particular, committee members, personnel from external bodies or persons acting on behalf of the certification body must keep all information received or generated during certification activities confidential, unless otherwise required by law (see ISO/IEC 17065:2012 subs. 6.1.1.3).

(4) A certification body provides public access to appropriate and timely information about its selection, determination, and certification activities, and about the certification status (granting, maintaining, extending or limiting the scope of certification, suspension, withdrawal or refusal of certification) of any data processing operation to generate confidence in the integrity and credibility of the certification (see ISO/IEC 17065:2012 subs. A.4.3). Openness is a principle for access to or disclosure of relevant information.

§ 3.1.5 Performing certification activities under non-discriminatory conditions

(1) The certification body ensures that the policies and procedures under which the certification body operates and its administration are non-discriminatory.

(2) The certification body ensures that activities by (outsourced) evaluators are performed in a non-discriminatory manner.

§ 3.1.6 Delimitation of responsibilities

(1) The certification body is responsible for fulfilling the certification requirements (see ISO/IEC 17065:2012 subs. A.6.1).

(2) If outsourced evaluators perform activities, the certification body is responsible for ensuring that all certification requirements contained in this scheme are fulfilled by the outsourced evaluators at all times.

(3) The cloud provider is responsible for fulfilling the certification criteria, not the certification body (see ISO/IEC 17065:2012 subs. A.6.1).

(4) The certification body is responsible for obtaining sufficient objective evidence on which to base the certification decision (see ISO/IEC 17065:2012 subs. A.6.2). Based on an evaluation of the evidence, it decides to grant a certificate if conformity is sufficiently demonstrated or not to grant a certificate if conformity is not sufficiently demonstrated.

§ 3.1.7 Openness to complaints

(1) The certification body is open to complaints from cloud providers or interested parties (see ISO/IEC 17065-1:2013 subs. 4.1.2.2, 4.6, 7.13). If these complaints are found to be justified, stakeholders should have confidence that the complaints will be dealt with in an appropriate manner and that reasonable efforts will be made by the certification body to resolve them (see § 4.3.2). Effective handling of complaints has an important role in protecting certification bodies, their clients and other users relying on certifications from errors, omissions or unreasonable behaviour. Confidence in certification activities is ensured when complaints are handled appropriately.

4 Requirements of a certification body

4.1 Basic certification requirements

§ 4.1.1 Accreditation of the certification body

(1) Certification bodies must tolerate accreditation by the DAkkS in accordance with ISO/IEC 17065 in conjunction with the supplementary requirements for accreditation pursuant to Art. 43 (3) GDPR and this scheme.

(2) The certification body may perform certifications under this scheme only if it has a valid accreditation.

(3) Certification bodies must be aware, that accreditation pursuant to Art. 43 (3) of the GDPR, will be limited to a maximum of five years (see DSK 'Duration of accreditation').

(4) In the event of suspension or withdrawal of accreditation (irrespective of how such a decision was reached), the following applies:

(a) A suspension (temporary withdrawal of accreditation) or withdrawal (permanent revocation of accreditation) of accreditation leads to the invalidity of the certifications awarded (see DSK subs. 4.1.2.2);
(b) The certification body must revoke the certifications it has issued insofar as they relate to the suspended or withdrawn accreditation (see IAF/ILAC A5:11/2013 subs. M.8.3.2.1., DSK subs. 4.1.2.2);
(c) In the certification agreement, it must be pointed out and bindingly regulated (see § 5.1.2) that the certification of the cloud provider is dependent on the accreditation of the certification body (see DSK subs. 4.1.2.2). In particular, the consequences of suspension or withdrawal of accreditation should be specified in the agreement;
(d) The certification body may then no longer make use of any advertising referring to its accredited status.

(5) Reasons for a suspension or withdrawal of the accreditation decision by the DAkkS can include (see DAkkS 71 SD 0 001 subs. 4):

(a) failure to meet essential accreditation requirements (e.g. personnel, facilities, premises);
(b) repeated or particularly serious violation of accreditation rules;
(c) deliberate deception of the accreditation body by providing false or incomplete information essential for the assessment of the certification body;
(d) failure to comply with conditions imposed even after a period of grace has been granted.

(6) Procedures for handling the suspension or withdrawal of accreditation are integrated into the management system of the certification body (see DSK subs. 4.1.2.2). To this end, the certification body must in particular establish processes to:

(a) immediately inform the certified cloud providers, cloud providers in an ongoing certification process, cloud providers which have submitted a certification application and other stakeholders inquiring about the AUDITOR certification about the suspension or withdrawal of accreditation and describe the consequences (see IAF/ILAC A5:11/2013 subs. M.8.3.2.1., DSK subs. 4.1.2.2);
(b) inform the scheme owner of the suspension or withdrawal of accreditation, as any rights of use and agreements with the certification body may be affected (see subsection 4.4);
(c) remove any advertising (e.g. on websites) related to the accreditation;
(d) initiate measures to restore accreditation and coordinate them with the DAkkS;
(e) establish and maintain a transfer policy for certifications issued (see DSK subs. 4.1.2.2) which:
    (i) establishes measures to transfer an issued certification within six months to a receiving certification body with valid accreditation;
    (ii) includes an up-to-date and continuously maintained register of accredited certification bodies which can undertake certification in accordance with a contractually concluded agreement;
    (iii) involve the DAkkS in the assessment of the transfer;
    (iv) informs the competent data protection supervisory authority of the transfer and involves it in the transfer if requested;
    (v) informs the scheme owner about the transfer;
    (vi) is stipulated by contract in the certification agreements (see § 5.1.2);

(vii) can be guided by the requirements of IAF MD 2:2017 for the transfer of accredited certification of management systems.

(7) Certification bodies will be informed, that re-accreditation following the five-year validity period of the accreditation is possible but must be completed successfully before the validity period expires so that any existing certification does not become invalid.

§ 4.1.2 Toleration of an on-site assessment during the accreditation process

(1) The accreditation body must tolerate the activities during the accreditation process, among others especially an on-site assessment by employees of the DAkkS and the competent data protection supervisory authority.

(2) Reference is made to the description of the accreditation process for the area of "data protection" according to Art. 42, 43 GDPR of the DAkkS as well as the DAkkS-rule 71 SD 0 00.

§ 4.1.3 Toleration of a witnessing audit during the accreditation process

(1) The certification body must tolerate a witnessing audit of the DAkkS and the competent data protection supervisory authority (see DSK subs. 6.1.2.1, 'Annex 2: Witnessing Model').

(2) Reference ist made to the description of the accreditation process for the area of "data protection" according to Art. 42, 43 GDPR of the DAkkS[1] as well as the DAkkS-rule 71 SD 0 013.

§ 4.1.4 Ensuring impartiality

(1) In order to ensure impartiality according to § 3.1.2, the certification body must continuously comply with all requirements of ISO/IEC 17065:2012 subs. 4.2.

(2) The certification body must have a mechanism to ensure its impartiality. To this end, the certification body complies with the requirements of ISO/IEC 17065:2012 subs. 5.2. In particular, continuous identification, documentation, assessment and elimination or mitigation of risks for the certification body, its personnel and related bodies is required (see ISO/IEC 17065 subs. 4.2.3, 4.2.4, DAkkS 71 SD 0 013 subs. 3.1).

(3) According to the requirements of the DSK, impartiality is only given if, in addition to the requirements under § 3.1.2, the certification body consistently complies with the following requirements (see DSK subs. 4.2.1):

(a) in accordance with Art. 43 (2) lit. a GDPR, separate evidence of the characteristic of independence must be submitted to the competent data protection supervisory authority as part of the accreditation process. In particular, the certification body has to submit evidence regarding its financing, insofar as it relates to ensuring impartiality, and evidence that its tasks and duties do not lead to a conflict of interest (see DSK subs. 4.2.1, 'Chapter 5', EDPB Annex 1 subs. 4.2);

(b) pursuant to Art. 43 (2) lit. e GDPR, the certification body must demonstrate to the competent data protection supervisory authority that its tasks and duties do not lead to a conflict of interest. Such conflicts could arise, for example, from a high dependence on turnover from clients or other economic pressure on the certification body (see DSK subs. 4.2.1, 'Chapter 5', EDPB Annex 1 subs. 4.2);

(c) in accordance with ISO/IEC 17065:2012, the certification body must also be a third party as defined in ISO/IEC 17000:2004. A third party is a body that is an independent party that assesses the certification object and is not a user of the certification object. According to the first sentence of Article R 17 (3) of Decision No 768/2008/EC, a certification body must be an independent third party which has no connection whatsoever with the entity it assesses. According to paragraph 4 of Article R 17 of Decision No 768/2008/EC, a certification body, its top-level management and the personnel responsible for performing the conformity assessment tasks must not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the products being assessed, or the authorised representative of any of those parties, unless that link does not compromise impartiality on grounds of minor relevance. The necessary impartiality and separation of the involved parties must be ensured and documented. A third party is *not* an entity that concludes contracts with certification clients. Thus, in particular, contracting authorities, contracting entities and their organisations which are or may be contractual partners cannot themselves be certification bodies. If the certification body is legally separate from such an organisation, the following paragraph (4) applies.

[1] https://www.dakks.de/content/projekt-datenschutz

(4) According to subs. 4.2.7 of ISO/IEC 17065:2012, the certification body is required to ensure that activities of legally separate legal entities with which the certification body or the legal entity to which it belongs has relationships do not affect the impartiality of its certification activities (see DSK subs. 4.2.7). A certification body that belongs to or is controlled by a legal entity (e.g. association or public body) or has other relationships with a legal entity whose members or shareholders are manufacturers, suppliers, processors or controllers certified by that certification body can only be considered an independent third party if its independence in accordance with Art. 43(2) (a) GDPR or impartiality according to subs. 3.13 of ISO/IEC 17065:2012 and absence of any conflicts of interest can be demonstrated. This may be the case if

(a) the certification body is legally separate from the legal entity, and
(b) the personnel of the certification body and the legal entity are separate and do not act in any way on behalf of the certification body, in particular in certification, testing and inspection procedures (see ISO/IEC 17065:2012 subs. 4.2.8), and
(c) the top management of the certification body commits itself to impartiality in the articles of association or in the statutes of the certification body, as defined in subs. 4.2.5 of ISO/IEC 17065:2012, and
(d) if the articles of association or statutes contain a section on the independence of the managing director and/or the head of the certification body from instructions, and
(e) in accordance with subs. 4.2.2 of ISO/IEC 17065:2012, there is no relationship of economic dependency with the members of the legal entity or the legal entity itself.

§ 4.1.5 Maintaining confidentiality

(1) In general, certification activities must be carried out confidentially. The certification body and its (outsourced) evaluators must therefore comply consistently with all requirements of ISO/IEC 17065:2012 subs. 4.5.

§ 4.1.6 Performing certification activities under non-discriminatory conditions

(1) The certification body and its (outsourced) evaluators must comply consistently with all the requirements of ISO/IEC 17065:2012 subs. 4.4 to ensure that the policies and procedures under which the certification body operates and its management are non-discriminatory.

§ 4.1.7 Legal responsibility

(1) The certification body must be a legal entity or a defined part of a legal entity so that the legal entity can be held legally responsible for all its certification activities (see ISO/IEC 17065:2012 subs. 4.1.1).
(2) A certification body should be able to demonstrate to the DAkkS or the relevant data protection supervisory authority that it has up-to-date procedures in place to demonstrate compliance with the legal responsibilities set out in the conditions of accreditation, including the additional requirements relating to the application of the GDPR (EDPB Annex 1 subs. 4.1.1).
(3) The certification body is also a controller or processor of personal data (e.g. data from the cloud provider) and must therefore be able to provide evidence of compliance with the procedures and measures under the GDPR specific to the control and handling of cloud providers' personal data as part of the certification process (EDPB Annex 1 subs. 4.1.1).

§ 4.1.8 Liability and financing

(1) The certification body must be able to demonstrate that it has assessed the risks arising from its certification activities and has adequate arrangements (e.g. insurance or reserves) in place to cover liabilities arising from its areas of activity in the geographical regions in which it operates (see ISO/IEC 17065:2012 subs. 4.3.1, DSK subs. 4.3, EDPB Annex 1 subs. 4.3).
(2) The certification body must have the financial stability and resources necessary for its activities (see ISO/IEC 17065:2012 subs. 4.3.2).
(3) The certification body has to prove its financial stability (see DSK subs. 4.3, EDPB Annex 1 subs. 4.2). The decision regarding the selection and designation of this documentary evidence is at the discretion of the DAkkS and the competent data protection supervisory authority. The evidence must be submitted annually (see EDPB Annex 1 subs. 4.3).
(4) The certification body must have adequate financial loss liability insurance for the scope of its activities (see DSK subs. 4.3, EDPB Annex 1 subs. 4.3). The calculation of the necessary coverage is based on a risk assessment of the certification body.

§ 4.1.9 Provision of information to the public

(1) The certification body must maintain a schedule of responsibilities (see DSK subs. 8.11.1),

(i) to handle requests for information from interested parties
(ii) to enable contact in the event of a complaint about a certification that has been granted.

(2) The certification body must maintain and make available (through publications, electronic media, or other means) the following information on request (see ISO/IEC 17065:2012 subs. 4.6):

(a) information about (or reference to) this conformity assessment scheme, including selection and determination procedures; rules and procedures for granting, maintaining, extending, limiting, suspending, withdrawing or refusing certifications;
(b) a description of the means by which the certification body receives financial support and general information on the fees charged to cloud providers;
(c) a description of the rights and obligations of cloud providers, including requirements, restrictions or limitations on the use of the certification name and its marks of conformity and how the certification is referred to;
(d) information on procedures for dealing with complaints and appeals in accordance with Article 43 (2) lit. d GDPR (see DSK subs. 4.6, EDPB Annex 1 subs. 4.6). This obligation to publish information refers not only to individual incidents, but also to the structure and procedure for handling complaints by the certification body.

4.2 Requirements regarding the structure and resources of the certification body

§ 4.2.1 Requirements regarding the organisational structure and top management

(1) The certification body must consistently comply with the requirements of ISO/IEC 17065:2012 subs. 5.1.
(2) The competent supervisory authority must be notified before a certification body starts operating an approved European Data Protection Seal from a satellite office in a new member state (see DSK subs. 7.1.2).

§ 4.2.2 Requirements regarding the personnel management of the certification body

(1) The certification body must employ or have access to a sufficient number of personnel to cover the staffing needs of its certification activities and to meet the certification requirements.
(2) The certification body must consistently comply with the requirements of ISO/IEC 17065:2012 subs. 6.1.

§ 4.2.3 Requirements regarding the competences of personnel

(1) Personnel must be competent for the tasks they perform, including carrying out the necessary professional assessments and establishing and implementing basic rules (see ISO/IEC 17065:2012 subs. 6.1.1.1).
(2) The requirements regarding the competences of personnel are defined by the supplementary requirements of the DSK in its definitive version, which must be met consistently by the certification body.
(3) The certification body is required to establish, implement, and maintain a procedure for management of the competences of personnel involved in the certification process (see EDPB Annex 1 subs. 9.2, DSK subs. 8.10). For this purpose, the certification body must consistently meet the requirements of ISO/IEC 17065:2012 subs. 6.1.2. This includes, in particular, keeping the knowledge of the personnel up to date in relation to evaluation and decision-making (see DSK subs. 6.1.2.1). The ongoing training of personnel, for example, with regard to the developments listed in § 4.5.2 therefore plays an important role in maintaining competence and must be carried out (see DSK subs. 8.10).

§ 4.2.4 Contract with personnel

(1) The certification body must consistently comply with the requirements of ISO/IEC 17065:2012 subs. 6.1.3.

§ 4.2.5 Integration regarding external resources (outsourcing)

(1) A certification body may appoint an outsourced, independent, and technically competent conformity assessment body or (individual) external evaluators to perform the selection and/or determination activities in accordance with ISO/IEC 17065:2012 subs. 6.2.2.
(2) The conformity assessment body and outsourced evaluators have a contractual relationship with the certification body. A contractual relationship must not exist with the cloud provider to be certified.
(3) The certification body must only outsource selection and determination activities to conformity assessment bodies and evaluators that comply with the certification requirements described in this conformity assessment scheme. In particular, the data protection-specific requirements for conducting certification must be met by the conformity assessment bodies and evaluators (see DSK subs. 6.1.2.1, 6.2.2).
(4) If the certification body outsources determination activities, the conformity assessment bodies and outsourced evaluators are required to be accredited in particular according to the relevant international standard (see ISO/IEC 17065:2012 subs. 6.2, 7.4.5), specifically ISO/IEC 17020 for inspection, ISO/IEC 17021 for auditing management systems, ISO/IEC 17025 for testing, ISO/IEC 17065 for certification.
(5) The certification requirements of the impartiality of personnel performing the selection and determination activities set out in this scheme are always applicable.
(6) The certification body must:

   (a) take responsibility for all activities outsourced to conformity assessment bodies and evaluators;
   (b) plan, control and monitor the performance of selection and determination activities;
   (c) have documented policies, procedures and records for the qualification, assessment and monitoring of all conformity assessment bodies and evaluators providing outsourced services used for certification activities;
   (d) maintain a list of approved conformity assessment bodies and evaluators of outsourced services;
   (e) implement corrective measures for any violations of the certification agreement and other requirements of this scheme by conformity assessment bodies and evaluators of which it becomes aware;
   (f) inform the cloud provider in advance of outsourced activities to give it the opportunity to object.

(7) If the qualification, assessment and surveillance of the conformity assessment bodies and evaluators providing outsourced services are carried out by other organisations (e.g. the DAkkS or competent data protection supervisory authority), the certification body may take such qualification and surveillance into account if:

   (a) the scope extends to the outsourced activities;
   (b) the validity of the specifications for qualification, assessment and surveillance is verified at regular intervals determined by the certification body.

(8) The certification body requires conformity assessment bodies and outsourced evaluators performing selection or determination activities to sign a contract or other document committing them to (see ISO/IEC 17065:2012 subs. 6.1.3):

   (a) comply with the policies and processes established by the certification body, including those relating to confidentiality and independence from commercial and other interests;
   (b) complete their work in a non-discriminatory, confidential, and impartial manner;
   (c) disclose any past and/or present affiliations on their part or on the part of their employer with:
      (i) a supplier or developer of products
      (ii) a provider or developer of services
      (iii) an operator or developer of processes

      related to the selection or determination activities of a cloud provider to which they are assigned; and
   (d) disclose any situation that may lead to a conflict of interests involving them or the certification body.

(9) Certification bodies must regard this information as a means of identifying threats to impartiality arising from the activities of the relevant personnel or the organisations that employed them.

(10) The certification body may, if necessary, establish a procedure for the approval of conformity assessment bodies and outsourced evaluators. In this case, the approval must be based on transparent, non-discriminatory, objective standards. Where the certification body carries out an approval procedure, it may stipulate that it will only accept certification assignments if the selection and/or determination activities are performed by conformity assessment bodies and evaluators approved by it.

§ 4.2.6 Requirements regarding internal resources

(1) The certification body must consistently comply with the requirements of ISO/IEC 17065:2012 subs. 6.2.1.

(2) In particular, if the certification body carries out the determination activities with its internal resources or with other resources under its direct control, it must be accredited according to the appropriate international standard (see ISO/IEC 17065:2012 subs. 6.2, 7.4.5), specifically ISO/IEC 17025 for testing, ISO/IEC 17021 for auditing management systems and ISO/IEC 17020 for inspection.

(3) If technical equipment (e.g. servers) and applications (e.g. software for performing technical tests) are used for the determination (possibly provided externally), the certification body is required to ensure that the measurement accuracy and/or measurement uncertainty necessary to provide a valid result are achieved. Suitability must be reviewed on an ongoing basis. The technical resources used must be maintained continuously and their operability ensured.

(4) When using information systems to perform certification activities, it must be ensured that procedures are in place and implemented to protect the integrity and security of the data.

4.3 Requirements regarding certification activities

§ 4.3.1 Records management

(1) The certification body must keep records to demonstrate that all certification requirements for the certification process have been effectively fulfilled (see ISO/IEC 17065:2012 subs. 7.12.1).

(2) In addition, the certification body must keep statistics on completed and aborted certification processes (see DSK subs. 7.12).

(3) All records must be kept complete, traceable, up-to-date and audit-proof (see DSK subs. 7.12). This applies both to completed certification processes, those terminated without a positive decision and ongoing certification processes. For ongoing certification processes, it must be possible to see which certification criteria have been met and which have not yet been met.

(4) The certification body must keep records confidential. The records must be transported, posted, or transmitted in a manner that ensures confidentiality (see ISO/IEC 17065:2012 subs. 7.12.2).

(5) Records must be kept at least for the current and the previous certification cycle (see ISO/IEC 17065:2012 subs. 7.12.3). With a certification validity period of 3 years (see § 5.5.5), the retention period is therefore at least 3 years at the start of a new cycle and a maximum of 6 years at the end of the current cycle. This period may be extended beyond the validity of the certification in the event of disputes between the certification body and the cloud provider or between the cloud provider and the competent data protection supervisory authority, until they have been resolved (see DSK subs. 7.12).

§ 4.3.2 Dealing with complaints and appeals within the certification process

(1) The certification body must have a documented procedure for receiving, evaluating and making decisions on complaints and appeals (see ISO/IEC 17065:2012 subs. 7.13.1, EDPB Annex 1 subs. 7.13, 9.3.3, DSK subs. 8.11.2).

(2) A complaint by any person or organisation denotes an expression of dissatisfaction about certification activities and requires a response from the certification body (see ISO/IEC 17000:2004 subs. 6.5).

(3) In contrast to a complaint, an appeal represents a request by the cloud provider to a certification body to review its decision regarding the certification object (see ISO/IEC 17000:2004 subs. 6.4).

(4) A complaint management system must be established as an integral part of the certification body's management system (see DSK subs. 8.11.3); in particular, it must consistently comply with the requirements of ISO/IEC 17065:2013 subs. 4.1.2.2 lit. c, 4.1.2.2 lit. j, 4.6 lit. d and 7.13.

(5) A description of the structure and process for handling complaints and appeals by the certification body must be publicly available to all interested parties (see ISO/IEC 17065:2013 subs. 4.6, 7.13, DSK subs. 4.6).

(6) The process for handling complaints and appeals must include at least the following activities and the certification body is required to ensure that appropriate measures are taken (see ISO/IEC 17065:2013 subs. 7.13):

  (a) procedures for receiving, validating, investigating the complaint or appeal, and deciding what measure to take in response;
  (b) activities to integrate the complaint management system of the respective cloud provider (see DSK subs. 4.1.2.2);
  (c) activities to record complaints or appeals, including measure taken to resolve them.

(7) The certification body should provide a contact form or equivalent that is easy to find and use on its website for making complaints.

(8) When receiving a complaint or appeal, the certification body confirms whether the complaint or appeal relates to certification activities for which the certification body is responsible and, if so, the certification body must address it and take any necessary follow-up measure to resolve the complaint or appeal (see ISO/IEC 17065:2012 subs. 7.13.2, 7.13.3, 7.13.9).

(9) The certification body is responsible for gathering and verifying all the information necessary (as far as possible) to reach a decision on the complaint or appeal (see ISO/IEC 17065:2012 subs. 7.13.4).

(10) The certification body must define appropriate deadlines for the parties involved and for the measures to be taken, according to the scope, range and criticality of the complaint or appeal, in order to manage the process of handling complaints and appeals in terms of time (see DSK subs. 7.13).

(11) The decision resolving the complaint or appeal is made or assessed and approved by a person (or persons) not involved in the certification activities relating to the complaint or appeal (see ISO/IEC 17065:2012 subs. 7.13.5, DSK subs. 7.13).

(12) To ensure that there is no conflict of interest, personnel, including those in a senior position, and those who have provided consultancy services to or are employed by a cloud provider within the last two years, must not assess or approve the resolution of a complaint or appeal (see ISO/IEC 17065:2012 subs. 7.13.6, DSK subs. 7.13).

(13) The certification body must explain how the separation of personnel between certification activities and the processing of appeals and complaints is ensured (see DSK subs.t 7.13).

(14) On request by the complainant, appellant or another party involved, the certification body must provide information on the current processing status of a complaint or an appeal (see DSK subs. 7.13).

(15) The certification body must formally inform the complainant or appellant and all other parties involved of the outcome and termination of the complaint or appeal procedure (see ISO/IEC 17065:2012 subs. 7.13.7, 7.13.8, DSK subs. 7.13).

(16) In the event of justified complaints, the certification body must inform the competent data protection supervisory authority (see DSK subs. 8.11.3).

(17) The certification body must record and retain complaints and appeals and the measures taken to resolve them. The retention period should correspond to at least one certification cycle. Individual incidents must be published in an appropriate manner (see DSK subs. 4.6).

(18) The scheme owner may be consulted to clarify complaints and appeals if, for example, there is confusion about certification requirements or criteria. The scheme owner must consider whether it can contribute relevant information or resources to clarify the situation. There is no obligation for the scheme owner to provide support.

§ 4.3.3 Management of changes to data processing operations

(1) The certification body requires the cloud provider to inform the body immediately of any changes that may affect the provider's ability to meet the certification criteria throughout the period of validity of the certification. The certification body is required to establish a process for receiving and handling such notifications from a cloud provider. Examples of changes are (see ISO/IEC 17065:2012 subs. 4.1.2.2):

(a) changes in legal, economic, or organisational status or ownership and changes in factual or legal circumstances (see DSK subs. 4.1.2.2);
(b) changes in organisation and management (e.g. changes in key positions, decision-making processes or technical personnel);
(c) substantial changes to software or hardware which are necessary for the provision of the data processing operations;
(d) substantial changes with regard to the processing of personal data;
(e) changes in the legal standards relevant to the certification object and in the state of the art of technology;
(f) changes to data centres (e.g. change of location);
(g) changes in the involvement of sub-processors with relevance to the data processing operation.

(2) The certification body is obliged to investigate the facts within four weeks and to take appropriate measures if information about such changes could have an influence on the conformity assessment statement (see DSK subs. 4.1.2.2). The certification body must also define how it ensures that comparable measures are taken in comparable cases. Appropriate measures are:

(a) use of determination methods (see § 5.2.4) to determine compliance with the certification criteria affected by the change (see ISO/IEC 17065:2012 subs. 7.11.1); in particular, the certification body may determine that an interim assessment is required to maintain certification. The requirements regarding an interim assessment according to § 5.6.4 must be met;
(b) the certification body may recommend re-certification with a different scope to the cloud provider (see § 5.6.9);
(c) if a non-conformity with certification criteria is detected, implementation of the measures described under § 5.6.4 in accordance with the requirements specified therein.

(3) The certification body must give the cloud provider the contact details of the person to whom the cloud provider can report changes to data processing operations and who is responsible for questions regarding the AUDITOR certification, at the latest when the certification agreement is settled (see DSK ADZ subs. 3).

§ 4.3.4 Management of changes to legal frameworks

(1) The certification body must consistently implement appropriate measures to identify changes in the legal framework affecting the body or the certification promptly. Examples of changes include (see DSK subs. 7.10, EDPB Annex 1 subs. 7.10):

(a) legislative amendments;
(b) adoption of delegated acts of the European Commission;
(c) decisions of the EDPB;
(d) court decisions;
(e) further developments in the state of the art of technology (as far as relevant for future certification and surveillance).

(2) The certification body must promptly inform the cloud provider of any changes to the legal framework that affect it or the certification (see DSK subs. 7.10).
(3) The certification body is obliged to determine the facts and to take appropriate measures in the event that such changes could have an influence on the conformity assessment statement (see DSK subs. 4.1.2.2). Appropriate measures are:

(a) determination methods (see § 5.2.4) to determine compliance with the certification criteria affected by the change (see ISO/IEC 17065:2012 para 7.11.1); in particular, the certification body may determine that an interim assessment is required to maintain certification. The requirements regarding an interim assessment according to § 5.6.4 must be met;
(b) the certification body may recommend re-certification with a different scope to the cloud provider (see § 5.6.9);
(c) if a non-conformity with certification criteria is detected, implementation of the measures described under § 5.6.4 in accordance with the requirements specified therein.

(4) The certification body must also define how it ensures that comparable measures are taken in comparable certification processes (also in the event of a change in the certification requirements) (see DSK subs. 7.10).

(5) The certification body must also inform the scheme owner if the changes have an impact on the certification requirements or criteria or are of major importance. If the scheme owner becomes aware of changes, it must inform the certification bodies accordingly (see § 2.1.4).

§ 4.3.5 Management of changes to this scheme

(1) The scheme owner may make changes to the established certification criteria, certification requirements and this scheme (e.g. due to changes in the legal framework). The scheme owner is then required to inform the certification body.

(2) If new or revised certification requirements are introduced under this conformity assessment scheme, the certification body undertakes to implement those requirements promptly. Where such changes also affect outsourced evaluators, the certification body informs the outsourced evaluators of the changes and ensures that the requirements are implemented within a reasonable time and thereafter consistently met by the outsourced evaluators.

(3) A certification body must establish appropriate processes to respond to changes in this scheme. These include, but are not limited to, the following measures:

(a) a certification body must inform a cloud provider of changes to the certification criteria or this scheme insofar as those changes affect the provider or its certification;

(b) a certification body must take measures to implement changes to certification requirements in a timely manner;

(c) the certification body is obliged to determine the facts for each certified data processing operation and to take appropriate measures if changes to certification criteria could have an influence on the conformity assessment statement. Appropriate measures are:

(i) determination methods (see § 5.2.4) to determine compliance with the certification criteria affected by the change (see ISO/IEC 17065:2012 para 7.11.1); in particular, the certification body may determine that an interim assessment is required to maintain certification. The requirements regarding an interim assessment according to § 5.6.4 must be met;

(ii) the certification body may recommend re-certification with a different scope to the cloud provider (see § 5.6.9);

(iii) if a non-conformity with certification criteria is detected, implementation of the measures described under § 5.6.4 in accordance with the requirements specified therein.

§ 4.3.6 Management of communication with the competent supervisory authority

(1) The certification body must establish procedures and responsibilities to involve the competent supervisory authorities in the necessary certification activities (e.g. appeals in relation to granting certification, see § 5.5.6).

(2) Enquiries from the supervisory authorities must be received, documented and answered promptly by the certification body.

4.4 Requirements regarding the use of this scheme

§ 4.4.1 Carrying out certifications in accordance with this scheme

(1) The scheme owner makes this scheme available on a non-discriminatory basis to interested certification bodies, in accordance with the requirements of Art. 101 and 106 TFEU (FRAND agreement).

(2) The scheme owner concludes a licence agreement with interested certification bodies (see ISO/IEC 17030:2009 subs. 4.3).

(3) The certification body confirms in this licence its agreement to comply with the requirements of this scheme (see ISO/IEC 17030:2009 subs. 7.2).

§ 4.4.2 Keeping a register of certified data processing operations

(1) The certification body maintains a publicly accessible register of certified data processing operations to enable traceability by interested parties (see ISO/IEC 17030:2009 subs. 5.3, subs. 7.1).

(2) For each certified data processing operation, information comprising at least the following details should be published at the time of certification (see ISO/IEC 17065:2012 subs. 7.8, DSK subs. 7.8, ISO/IEC 17030:2009 subs. 5):

(a) a clear designation of the certification object;

(b) a clear designation of the cloud provider, including the name and address of the cloud provider;
(c) the certification body, logo of the certification body if applicable;
(d) the definitive version of the AUDITOR Criteria Catalogue according to which conformity was certified;
(e) the name of the relevant version of the conformity assessment scheme;
(f) a certification number;
(g) the validity period of the certification, including date of decision and end of certification;
(h) the certification statement that the certified data processing operations meet the relevant requirements of the GDPR and the BDSG in accordance with the AUDITOR Criteria Catalogue in its latest version for a specific protection category and specific restorability class;
(i) Information about the initial certification and re-certification (e.g. date of initial certification, number of re-certifications);
(j) information about any involvement of outsourced evaluators;
(k) point of contacts for complaints, for example in the event of discovery of non-conformity;
(l) a brief indication of monitoring activities to maintain certification;
(m) a short report on the certification results, from which the exact certification object (including version or functional status), the evaluation procedure (including the criteria on which the certification is based (with version information if applicable) and an indication of criteria that were not applicable) and the evaluation result can be deduced (see DSK subs. 7.8).

(3) On request, the certification body must be able to provide timely information to interested parties explaining the meaning of the mark of conformity and whether a mark of conformity that has been issued remains valid (see ISO/IEC 17030:2009 subs. 7.1). Questions or concerns of interested parties regarding the mark of conformity must be dealt with in a timely and expedient way.
(4) All information must be stored in an electronic directory that is accessible via the internet and can be viewed by the general public. This electronic directory should be easy to access (e.g. without prior registration).
(5) The certification body must inform the scheme owner how to access the directory (e.g. communication of the internet address).

§ 4.4.3 Use of AUDITOR marks of conformity

(1) The certification body stipulates by legally enforceable agreements that the cloud provider may use the marks of conformity issued on websites, in (printed) publications, documents, and other promotional materials (see ISO/IEC 17030:2009 subs. 5.6), provided that no misunderstandings, ambiguities or misleading statements come about and all provisions of this scheme and any requirements of the licence agreement between the certification body and the scheme owner are observed.
(2) In particular, if a mark of conformity refers only to certain data processing operations of a cloud service or there are other restrictions on the scope (e.g. certain locations), the certification body must oblige the cloud provider to ensure in its communications that there is no misunderstanding and it is clear that the mark does not refer to the entire cloud service, all locations or other areas (see ISO/IEC 17030:2009 subs. 5.5).
(3) Affixing of marks of conformity to products or product packaging is not permitted (see ISO/IEC 17030:2009 subs. 5.4).
(4) The certification body must take appropriate measures to ensure that marks of conformity issued comply with the requirements of the scheme (see ISO/IEC 17065:2012 subs. 4.1.3).
(5) The certification body must take measures to minimise misunderstandings, ambiguities and misleading statements regarding the marks of conformity that could reduce their effectiveness (see ISO/IEC 17030:2009 subs. 4.2).
(6) The certification body must establish procedures for surveillance of correct use of the mark of conformity for the certification validity period (see ISO/IEC 17030:2009 subs. 4.2, 7.2, 7.3). These include in particular:

(a) sample assessment of the correct advertising of the marks of conformity at the time of initial issue;
(b) provision of a means of contact (e.g. contact form, e-mail address, etc.) for reporting unlawful or incorrect use of marks of conformity by interested parties;
(c) measures to resolve all complaints concerning the use of the mark of conformity, and recording of these measures;
(d) sample review of correct use as part of surveillance;

(e) measures to address misuse of the mark of conformity, including requests for correction and corrective measures, suspension and withdrawal of certifications, publication of the misuse or appropriate legal measure. This includes misuse of the mark of conformity by a party that does not have a contract with the certification body;

(7) Incorrect reference to or misleading use of marks of conformity found in publications or other publications must be reported to the scheme owner.

§ 4.4.4 Reporting to the scheme owner

(1) The certification body is obliged to send the scheme owner a short report on the operation of the scheme for scheme improvement at least once a year. This report must contain at least the following information:

(a) the number of certified data processing operations;
(b) a brief summary of significant reasons for complaints and appeals;
(c) a brief summary of the main reasons for discovery of non-conformity with the certification criteria;
(d) any outstanding issues or points requiring clarification in relation to this scheme;
(e) any suggestions for improving the scheme.

§ 4.4.5 Advertising with and reference to this scheme

(1) Certification bodies and certified cloud providers may refer to this scheme, provided that no misunderstandings, ambiguities or misleading statements come about.
(2) Reference should be made to the public registrations for this scheme with the DAkkS repositories or the website of the scheme owner.
(3) The authoritative version of the conformity assessment scheme and a reference date must be indicated.
(4) In case a reference is made the scheme owner is to be informed informally (e.g. by e-mail) in a timely manner (within 14 days).

4.5 Management system requirements

§ 4.5.1 Establishment of a management system

(1) The certification body must establish and maintain a management system that consistently meets the requirements of ISO/IEC 17065:2012 subs. 8.1 in accordance with either Option A or Option B and document, evaluate, control and self-monitor its application (see DSK subs. 8.1, 'Chapter 8 ', EDBP Subs. 8). Regardless of the option chosen, the management system must fulfil the requirements of this scheme. For this purpose, processes according to the previous sections must be implemented in the certification body's own management. This includes in particular (see DSK subs. 8.1.1):

(a) surveillance, control, evaluation and improvement of the structure of the internal processes of the certification body with ongoing collection of internal evidence;
(b) management of the expiry or revocation of the accreditation and prompt notification of the certified cloud providers of this (see EDPB Annex 1 subs. 9.3.4);
(c) complaint management administration;
(d) suspension and withdrawal of certification, with documentation of the reasons;
(e) contract management;
(f) ensuring independence (impartiality/financial stability) and managing the relevant evidence;
(g) publication of certification decisions etc.;
(h) resources (competence of personnel and external resources);
(i) application management;
(j) surveillance of changes affecting certifications;
(k) surveillance of the use of marks of conformity issued.

(2) For this purpose, the management system must provide a methodology for the way in which these requirements can be achieved and controlled in compliance with data protection and the way in which they can also be continuously reviewed by the certification body itself (see DSK 'Chapter 8').
(3) These management principles and their documented implementation must be comprehensible and must be disclosed by the certification body during the accreditation procedure and at any time thereafter at the request of the data protection supervisory authority, for example,

during an investigation in the context of data protection reviews (Art. 58 (1) (b) GDPR) or a review of certifications granted under Art. 42 (7) GDPR (Art. 58 (1) lit. c GDPR) (see DSK 'Chapter 8').

§ 4.5.2 Update of the evaluation methods

(1) The certification body must establish procedures to update the evaluation methods (see ISO/IEC 17065:2013 subs. 7.4, DSK subs. 8.9, EDPB Annex 1 subs. 9.1). Updates are required in the context of changes in the legal framework, the relevant sources of risk, the state of the art of technology and the implementation costs of TOM.

(2) The procedures must define the necessary steering measures (see DSK subs. 8.9.2) to ensure that:

(a) any relevant changes to the regulatory framework (as per ISO/IEC 17065:2013 subs. 7.4 and the associated extensions in this scheme),
(b) contractual components between cloud provider and certification body,
(c) all relevant emerging (categories of) sources of information technology risk and vulnerabilities and
(d) the progress of the state of the art of technology with regard to processing activities and technical and organisational measures that may be applied to ensure compliance with legal requirements, in particular with regard to the implementation of data protection principles and the security of processing,

are recorded, documented, assessed and reflected in the evaluation methods.

(3) Changes or change processes and their reasons must be documented to enable traceability (see ISO/IEC 17065:2013 subs. 7.10, DSK subs. 8.11.2).

(4) In addition, it must be ensured that changes to the requirements of the data protection supervisory authority and the EDPB for criteria catalogues and certification processes are monitored and that these changes are integrated promptly into the certification body's own procedures (see DSK subs. 8.9.2). Coordination with the scheme owner may be required in these cases. The accreditation body and the competent data protection supervisory authority must be informed of changes.

(5) The certification body must also ensure that legal acts and requirements of the EDPB or data protection supervisory authorities are handled promptly and implemented (see DSK subs. 8.9.2). The accreditation body and the competent data protection supervisory authority must be informed of this.

(6) Documentation on updating evaluation methods must be disclosed to the competent data protection supervisory authority on request (see DSK subs. 8.11.2).

5 Requirements regarding the certification process

The AUDITOR certification process comprises the sequential stages of selection (No. 5.1), determination (No. 5.2), review (No. 5.3), decision (No. 5.4) and attestation (No. 5.5). This is followed by continuous surveillance activities (No. 5.6).

No. 5.1 During the **selection** stage, evaluators carry out planning and preparatory activities to collect or provide all necessary information and inputs for the subsequent determination activities, including description and delineation of the certification object (see ISO/IEC 17000:2004 subs. A.2.1).

No. 5.2 The **determination** activities involve one or more determination methods (e.g. document review or audit) performed by evaluators to obtain complete information about the compliance of the data processing operations or samples of them with the certification criteria specified in the AUDITOR Criteria Catalogue (see ISO/IEC 17000:2004 subs A.3.1).

No. 5.3 By means of a **review,** the decision-makers verify whether the selection and determination activities and their results are suitable, appropriate and effective for assessing whether the data processing operations fulfil the certification criteria (see ISO/IEC 17000:2004 subs. A.4).

No. 5.4 The decision-makers subsequently make a **decision** whether to grant certification, based on the determination and review activities (see ISO/IEC 17000:2004 subs. 5.2).

No. 5.5 During **attestation,** the certification body issues the AUDTOR marks of conformity as evidence that compliance with the specified requirements has been demonstrated (see ISO/IEC 17067:2013 subs. 5.1.1).

No. 5.6 **Surveillance** comprises systematic, repeated conformity assessment activities as a basis for maintaining the validity of the conformity statement (see ISO/IEC 17000:2004 subs 6.1).

5.1 Selection

§ 5.1.1 Processing and review of the certification application

(1) The cloud provider is entitled to apply for certification as a data processor (see DSK point 7.2).

(2) The certification body must establish a process for evaluating the acceptance or rejection of applications for certification. The reasons for rejection must be specified to prevent any arbitrary decisions in the evaluation (see ISO/IEC 17065:2012 subs. 4.4.3). Possible reasons for rejection include cases in which:

(a) the cloud provider is involved in illegal activities;
(b) the cloud provider has repeatedly violated the AUDITOR certification criteria;
(c) similar cloud provider-related problems are demonstrably present.

(3) The certification body must refuse to carry out a particular certification

(a) if it lacks the competence or capability for the certification activities (see ISO/IEC 17065:2012 subs. 7.3.4);
(b) if it lacks the resources to carry out all selection and determination activities;
(c) if its impartiality is at risk.

(4) Acceptance of a certification application is not dependent on the size of the cloud provider or membership of an association or group, nor on the number of certifications already granted (see ISO/IEC 17065:2012 subs 4.4.3). There must be no unfair financial or other conditions.

(5) The certification body does not evaluate applications for a specific protection category or restorability class. This choice is the sole responsibility of the cloud provider.

(6) The certification body must keep records of the reasons for the decision to accept or reject an application for certification.

§ 5.1.2 Certification agreement

(1) The certification body must have a legally enforceable certification agreement with the cloud provider for the provision of certification activities (see ISO/IEC 17065:2012 subs 4.1.2).

(2) The certification body must establish and implement processes for concluding, amending and monitoring certification agreements (see DSK subs. 7.2, 7.3).

(3) The certification agreement defines the definitive version of the AUDITOR Criteria Catalogue.

(4) The certification agreement establishes this scheme as the governing procedural regulation, in particular regarding the granting, refusal, suspension, restriction, surveillance, and withdrawal of certification (see EDPB Annex 1 subs. 4.1.2).

(5) The certification agreement must include and clearly delineate the responsibilities of the certification body, any outsourced evaluators involved and the cloud provider (see ISO/IEC 17065:2012 subs 4.1.2).
(6) The certification agreement stipulates the cooperation obligations of the cloud provider (see § 5.1.3).
(7) The certification agreement contains a precise description of the certification object and the requested protection category and restorability class (see § 5.1.4).
(8) The certification agreement lists the certification criteria which cannot be applied to the specific certification object, insofar as these are already known (see § 5.1.5). The non-applicability must be justified.
(9) If the cloud provider seeks recognition of existing certificates for components of its data processing operations (see § 5.1.7), these certificates must be included in the agreement with a precise designation of the certificate to be recognised and the component of its data processing operations for which recognition is required.
(10) The planned methods of determination are contractually recorded in the certification agreement (see DSK point 7.4).
(11) If the certification body commissions outsourced evaluators to perform the determination activities according to ISO/IEC 17065:2012 subs. 6.2.2, this is documented in the agreement.
(12) The certification agreement describes the consequences of the suspension or withdrawal of the accreditation of the certification body according to § 4.1.1. The withdrawal of an accreditation has consequences for the cloud providers as clients of the certification body. It must therefore be pointed out in the certification agreement and regulated in a binding manner that the certification of the cloud provider is dependent on the accreditation status of the certification body. Suspension or withdrawal of that accreditation invalidates the certification (see DSK subs. 4.1.2.2, EDPB Annex 1 subs. 4.1.2).
(13) The certification agreement describes the concept for the transfer of certifications in the event of expiry of accreditation within the meaning of Art. 43 GDPR (see § 4.1.1), including the assessment of the transfer by the DAkkS (see DSK subs. 4.1.2.2).
(14) The certification agreement regulates the publication of information pursuant to Art. 42 (8) and Art. 43 (5) GDPR by the certification body (see EDPB Annex 1 subs. 4.1.2).
(15) The certification agreement stipulates that a cloud provider is required to provide the competent data protection supervisory authority with full access to the documentation of the certification process, including confidential information about compliance with the certification criteria (see EDPB Annex 1 subs. 4.1.1). The cloud provider must recognise the tasks and powers of the competent supervisory authority without prejudice (see EDPB Annex 1 subs. 4.1.1).
(16) The certification body must ensure that its certification agreement requires the cloud provider to comply at least with the following requirements (see ISO/IEC 17065:2012 subs. 4.1.2):

(a) to fulfil the certification criteria consistently (see DSK subs. 4.1.2.2, EDPB Annex 1 subs. 4.1.1), including implementation of appropriate changes when notified by the certification body (see ISO/IEC 17065:2012 subs. 4.1.2.2);
(b) to make all necessary arrangements for
    (i) performing determination activities and regular surveillance (in accordance with the arrangements for surveillance activities in No. 5.6), including consideration of the review of documentation and records, access to relevant equipment, the site(s), area(s) and personnel, and the cloud provider's sub-processors (see ISO/IEC 17065:2012 subs. 4.1.2.2, DSK subs. 4.1.2.2);
    (ii) (where applicable) the participation of observers (e.g. accreditation assessors or auditors in training);
    (iii) the investigation and handling of complaints (see ISO/IEC 17065-1:2013 subs. 7.13). Specific details about the structure and procedure for the cloud provider's complaint management, in particular means for integrating the complaint management with the certification body (see § 4.3.2), must be specified in the certification agreement (see DSK subs. 4.1.2.2, EDPB Annex 1 subs. 4.1.2).
(c) *not* to use the certification and marks of conformity in any way that might bring the certification body or scheme owner into disrepute, and *not* to make any statements about certification that the certification body or scheme owner might consider misleading or unwarranted;
(d) in the event of suspension, restriction, withdrawal or termination of certification, to discontinue the use of all promotional materials containing any reference to certification and take any measure required by this scheme and any other measure specified by the certification body;

(e) when referring to their certification in communication media, such as documents, brochures or promotional materials, to comply with the requirements of the certification body and the requirements laid down in § 5.5.2 to use marks of conformity;
(f) to keep records of all complaints made to the cloud provider regarding compliance with the certification criteria for at least the validity period of the certification and make those records available to the certification body and the competent data protection supervisory authority on request; and
    (i) take appropriate measures in relation to such complaints and any deficiencies discovered in the data processing operations that affect compliance with the certification criteria;
    (ii) document the measures taken.
(g) to inform the certification body without delay of any changes that might affect its ability to meet the certification criteria (see § 4.3.3, EDPB Annex 1 subs. 4.1.2). Examples of changes are given in § 4.3.3
(h) to observe and comply with those deadlines and process steps resulting from this conformity assessment scheme or other regulations (see DSK subs. 4.1.2.2);
(i) to provide cloud users, on request, with sufficient information about the certified protection category and restorability class, including a justification for the selection of the appropriate protection or restorability class.

(17) Certification bodies may charge reasonable fees for their activities. The fees are to be specified in the agreement with the cloud provider. The cloud provider must undertake to provide the cooperation required for proper certification or, if applicable, the contractually agreed cooperation at its own expense.
(18) The expected duration of the certification process is agreed between the parties involved and recorded in the agreement (see DSK point 4.1.2.2).
(19) If the agreement is changed after the certification activities have started, the contract review must be repeated. Any changes must be made known to all persons concerned (i.e., the certification body), any outsourced evaluators and the cloud provider.

§ 5.1.3 Cooperation obligations of the cloud provider

(1) The certification body requires that the cloud provider, within the scope of its responsibilities for the data processing operations, ensures that the certification body has access to mandatory information and data and - insofar as is necessary - access to data processing facilities of all kinds to carry out the certification activities.
(2) In particular, the certification body requires the cloud provider to provide the following information (see ISO/IEC 17065:2012 subs 7.2):

(a) a request to be certified according to the AUDITOR Criteria Catalogue and this scheme;
(b) the protection category and restorability class requested by the cloud provider;
(c) cloud provider details, including name and address(es) of locations;
(d) general information regarding the applicant cloud provider relevant to the certification area applied for, such as its activities, human and technical resources, organisational chart, market orientation (national, EU, international, selected markets in countries, etc.) and relationships to any larger body, if applicable;
(e) a comprehensive description of the certification object according to § 5.1.4;
(f) a comprehensive explanation of the non-applicability of certification criteria according to § 5.1.5;
(g) a comprehensive explanation of fulfilment of the certification criteria according to § 5.1.6
(h) whether consultancy services have been provided by the certification body in relation to the data processing operations to be certified and, if so, by whom and when.
(i) contact details of the contact for AUDITOR certification (see DSK ADZ subs. 3).

(3) The certification body sets a reasonable deadline for the cloud provider to provide all information (usually two to three months). The certification body obliges the cloud provider to provide all information promptly according to the milestones, deadlines or other points in time specified in the certification plan (see EDPB Annex 1 subs. 4.1.2).
(4) In the course of the certification process, the certification body may request further information and/or documentation which it considers necessary for certification. The certification body obliges the cloud provider to provide this information.

§ 5.1.4 Description and definition of the object of certification

(1) The object of certification (see ISO/IEC 17000:2004 subs. A.2.2) is data processing operations involving personal data in cloud services, see § 2.2.8.
(2) The certification body must ensure that the cloud provider has given sufficient information for assessment, delimitation and conclusive definition of the object of certification (see DSK ADZ subs. 2.1.2). In addition, the cloud provider must help to resolve any ambiguities in the event of queries. The documentation supplied by the cloud provider must at least contain a detailed description of the object of certification, which includes

(a) a designation and detailed (functional) description of the data processing operation or operations within the relevant cloud service to be certified;
(b) a detailed description of all components of the relevant data processing operations so that a closed structure is ensured;
(c) documentation of responsibilities of the cloud provider in the data processing operation;
(d) which data is processed in the connection of the object of certification (see DSK ADZ subs. 2.1.2) and
    (i) which data relates to special categories of personal data pursuant to Art. 9;
    (ii) which data relates to criminal convictions and offences pursuant to Art. 10;
(e) designation and information relating to sites where data processing operations are carried out (including identification of the head office and other sites and description of activities, risks per site, legal and contractual arrangements for each site, the degree of centralisation of processes/activities provided to all sites, the interfaces between the different sites (see IAF MD 1:2018 subs. 7.1));
(f) information regarding all outsourced operations used by the cloud provider as part of the data processing operation that affect compliance with the certification criteria. In particular, sub-processors and the responsibilities and associated tasks in relation to them must be named (see DSK point 7.2);
(g) a description of the interfaces with and transitions to other systems and organisations/sub-processors (e.g. in the form of a network plan). The underlying records (e.g. surveillance protocols, (template) contracts, agreements, guarantees) and other assurances must also be presented (see DSK point 7.2);
(h) indication of whether personal data is transferred
    (i) outside the European Union or the European Economic Area, or
    (ii) to international organisations (see DSK ADZ subs. 2.1.2).
    It must be noted that in practice, such third-country transfers often occur when transferring data in the context of maintenance, servicing and support (see DSK ADZ subs. 2.10). In particular, these activities may be carried out in exceptional cases and must therefore be considered during the certification process.
(i) the TOM of the cloud provider within the meaning of Art. 28 GDPR;
(j) the technology and IT landscape used, including relevant IT systems, and the interaction between technology and organisational processes;
(k) organisational processes for carrying out the data processing operations;
(l) the specific data protection risks to which the data processing operations are exposed.

(3) The certification body documents the exact definition of the certification object and makes this available to the cloud provider for cross-checking.
(4) The certification body provides adequate information about the certification object to the public on request, while maintaining confidentiality. The aim of disclosure is to create transparency regarding the specific certification object, as cloud services are complex.
(5) The certification body and the cloud provider can refer to the accompanying document *'AUDITOR certification object'* to assist in defining the object.

§ 5.1.5 Non-applicability of certification criteria

(1) For the specific and individual certification object (i.e. the specific cloud service to be certified and its processing operations) must be established, whether individual certification criteria are not applicable. Therefor the certification body initially requires the cloud provider to perform an assessment which certification criteria are applicable depending on each specific certification object. The cloud provider documents the identification of non-applicable certification criteria and informs the certification body of them. The documentation should contain as a minimum:

(a) a list of the criteria that are not applicable;

(b) a detailed justification per criterion why it is not applicable to the specific certification object.

(2) The certification body establishes a process for assessing and documenting the non-applicability of certification criteria. The certification body reviews the documentation supplied by the cloud provider about non-applicability for correctness and completeness. In particular, the certification body must ensure that the assessment of non-applicability relates to the specifics of a specific certification object (i.e. the cloud service to be certified and its processing operations) and that same decision regarding non-applicability is made for comparable certification processes and circumstances in order to prevent the possibility of arbitrariness. A global or generalised establishment of non-applicability of criteria is not possible. In particular, a free or arbitrary selection of criteria and the establishment of non-applicability should be prevented.

(3) If the non-applicability of a criterion is confirmed by the certification body, this criterion is not assessed within the scope of the determination activities. The certification body documents the verifiable reasons, decision-making rules and extent of non-applicability and the results of the review.

(4) If the certification body has doubts about the non-applicability of a criterion, the certification body attempts to resolve the ambiguities. For this purpose, further documents and explanations can be requested from the cloud provider, or determination methods (see § 5.2.4) can be used by the certification body.

(5) Criteria are not applicable

(a) if the cloud provider cannot perform them because they are outside its area of responsibility. For example, the cloud provider is obliged to assist the cloud user in providing information according to criterion no. 6.2. However, the criterion does not apply to the cloud provider's data processing operations, thereby exempting the cloud provider from providing information if the cloud user is responsible for the data in question and determines the applications and files (for example, in the case of Infrastructure-as-a-Service). The same applies if it is not the cloud provider but the sub-processor who is responsible for access to data processing systems pursuant to No. 2.3. In this case, criterion No. 2.3 does not apply to the cloud provider. The cloud provider must, however, assure itself that the sub-processors comply with the data protection regulations applicable to them (see no. 10.4) and that they therefore comply with criterion No. 2.3.

(b) if the cloud provider does not carry out the tasks described in the criteria. If, for example, the cloud provider does not involve sub-processors or if no data are processed outside of the EU or the EEA, the criteria in Sections V and VI are not applicable.

(c) if the General Data Protection Regulation or the laws that implement it do not absolutely require their applicability but make their applicability dependent on certain conditions or "thresholds" that are not met by the cloud provider. This is, for instance, the case when designating a data protection officer (Art. 37 (1) and (4) GDPR in conjunction with Sec. 38 BDSG) or when maintaining a record of processing activities (Art. 30 (5) GDPR).

(d) if the fulfilment of the criterion prevents a legitimate purpose of the data processing from being achieved. For example, a provider of an e-mail service cannot anonymise the mail headers, since otherwise the delivery of e-mails cannot be guaranteed, with the result that it cannot be required to carry out such an anonymisation.

(6) If the cloud provider or the certification body determines that certification criteria are not applicable due to the specific circumstances and characteristics of the data processing operation (e.g. when determining the object of certification or during determination and review activities), this must be justified, explained in detail and documented.

§ 5.1.6 Statement regarding fulfilment of the certification criteria

(1) The certification body requests a detailed statement from the cloud provider regarding fulfilment of the certification criteria to prepare and carry out subsequent determination activities.

(2) A statement should present correctly and completely for each certification criterion how the cloud provider implements the criterion. There should be separate explanations for the sub-items of the respective criterion (e.g. explanation for criterion No. 2.2 (2)). Furthermore, the statement may contain a reference to the corresponding documentation (e.g. process documentation, logs, intranet, wiki, etc.) or systems.

(3) The certification body may offer an electronic template for statements to assist cloud providers.

(4) The cloud provider assures the certification body that the measures mentioned in the statement have been fully implemented.

§ 5.1.7 Recognition of existing certificates

(1) If the cloud provider seeks recognition of existing certificates for components of its data processing operations, the certification body must immediately examine whether and to what extent recognition can be granted.

(2) There are only three possibilities within the certification process for recognising other certificates (see DSK ref. 7.4, ISO/IEC 17065:2012 ref. 6.2.2.4):

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

(3) A complete certification report (including a report about determination activities and their findings) is necessary for an assessment of the recognition. 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). A certificate or similar marks of conformity are not sufficient in this regard.

(4) Furthermore, the documentation for the existing certificate must contain a precisely described certification object and a description of the interfaces with or transitions to other systems and organisations (e.g., ISO/IEC 27001 Statement of Applicability, SoA).

(5) 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).

(6) Certifications underlying the certificate must be completed at the time of application (see DSK point 7.4).

(7) If the certification body recognises certificates for components of data processing operations, a complete assessment of these components is not required. However, the certification body must validate ongoing compliance with the criteria (of the submitted certificate) at least on a sample basis for critical evaluation of existing certificates.

(8) An assessment of the interaction of the recognised component of the data processing operation with other components, in particular the interfaces relevant to this interaction, is also required.

(9) If irregularities arise within the scope of AUDITOR certification with regard to recognised certificate (e.g. presumption 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).

(10) The certification body must justify and sufficiently document recognition, in particular regarding the protection category and the restorability class. It must be documented how and to what the recognition takes place and what concrete effects this has on the remaining scope of determination and the determination activities (see DSK subs. 7.4).

(11) The certification body must note the validity period and expiry date of the recognised certificates and keep them for the decision (see § 5.5.5). The ongoing validity of the recognised certificate is checked by the certification body at least as part of its surveillance activities. In addition, the certification body obliges the cloud provider to inform it with sufficient time in advance if a recognised certificate loses its validity as scheduled (i.e., at the regular expiry of the validity period) or in an unscheduled way (i.e. before the end of the regular validity period noted by the certification body) and what measures the cloud provider wants to take (e.g. re-certification). If the cloud provider does not seek re-certification of the recognised certificate, at least the area originally covered must be reassessed by the certification body to maintain the validity of the AUDITOR certification.

(12) When considering recognition, the certification body has to assess the material and procedural equivalence of the results of conformity assessments to ensure an equal level of confidence in conformity (see DSK subs. 7.4, ISO/IEC 17000:2004 subs. 7.4):

(a) A material equivalence exists if the other certificate is based on certification criteria that are comparable to or exceed those of the AUDITOR catalogue of criteria regarding the level of protection. The certification body determines the protection category and restorability class under which the certificate is recognised.

(b) A procedural equivalence exists if the other certificate was issued based on an accredited certification process that offers a comparable guarantee for proper determination and certification activities.

As a general rule, certificates issued by an accredited certification body, and thus in particular approved data protection certifications according to Art. 43 GDPR, are equivalent. There are no effects on the period of validity of the submitted certificates.

(13) Other certificates issued which are not covered by (2) cannot be recognised within the scope of the AUDITOR certification.

(14) Other certificates and their results reports can only be submitted by the cloud provider and, if appropriate, reviewed by the certification body during its determination activities. However, compliance with the AUDITOR certification criteria must be fully verified by the certification body by means of other suitable determination methods.

(15) 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 appropriate. 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 recognition within the framework of AUDITOR certification. In particular, the possibilities of recognition 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.

(16) Further information is also provided in the supplementary document *'AUDITOR Concept of Modularity'*.

§ 5.1.8 Evaluation of the information and documentation provided by the cloud provider

(1) The certification body carries out an assessment of the information received by the cloud provider (commonly known as "stage 1 auditing") to ensure that (see ISO/IEC 17065:2012 subs 7.3.1):

(a) the information about the cloud provider and the data processing operation is sufficient to carry out the certification process;
(b) the certification body is able to arrive at a sufficient understanding of the data processing operation;
(c) all known differences in understanding between the certification body and the cloud provider have been resolved;
(d) the certification object and scope of the certification are defined;
(e) the resources are available to carry out all selection and determination activities;
(f) the certification body has the technical and legal competence and ability to perform the requested certification activities for the cloud provider's individual certification object. In the absence of experience with the certification object or the cloud service type, the certification body must demonstrate both technical and legal competence for the certification activities of the individual request to an appropriate extent (see DSK subs. 7.3, EDPB Annex 1 subs. 7.3).

(2) The certification body must draw the attention of the cloud provider to the further types of information and records that may be required for a detailed determination in accordance with section 5.2 (commonly known as a "stage 2 auditing").

(3) If information cannot be provided to the certification body because it is confidential or sensitive, the certification body determines whether the data processing operation can still be adequately assessed. If the certification body concludes that it is not possible to assess the data processing operation adequately without reviewing the identified confidential or sensitive information, it advises the cloud provider that the certification process cannot proceed until appropriate access has been agreed and a confidentiality agreement has been reached.

(4) The certification body has the right to suspend or cancel the certification process if the cloud provider does not comply with the obligation to provide information and/or documentation (see DSK subs. 7.4).

5.2 Determination

§ 5.2.1 Calculating the time required for determination activities

(1) The certification body must have documented procedures for calculating the time required for performing determination activities (see ISO/IEC 17065:2013 subs. 7.4.1). In particular, the certification body must calculate for each cloud provider the time required to plan and conduct a complete and effective determination.
(2) The determination time should be as short as possible to facilitate certification of small and medium-sized cloud providers (within the meaning of Art. 42 (1) GDPR). At the same time, the scope and depth of the determination activities must be as great as possible to ensure the validity of the protection statement in the AUDITOR certification and compliance with the requirements of the General Data Protection Regulation.
(3) The duration of the determination activities and its justification must be recorded.
(4) The specified determination period can be extended if, for example, particular findings were made during the determination activities (e.g. the need for examination of additional locations, greater complexity of the data processing operations than originally envisaged) or if subsequent checks are necessary.
(5) Appendix A: Definition and calculation of the determination time provides binding guidelines for calculation of the time required.

§ 5.2.2 Planning the determination activities

(1) The evaluators prepare a determination plan prior to carrying out the determination activities (see ISO/IEC 17065:2012 subs. 7.4.1), which includes as a minimum information about the time schedule and the determination methods to be used. The determination plan is submitted to the cloud provider.
(2) The certification body designates personnel to carry out each determination task it performs with its internal resources (see ISO/IEC 17065:2012 subs 7.4.2).

§ 5.2.3 Objects of determination

(1) The determination is made on the basis of the clearly defined description of the certification object. The entire certification object, including all technical and organisational processes or series of processes, must comply with the applicable certification criteria of the AUDITOR Criteria Catalogue in the relevant version.
(2) The subject of the determination activities is also the interaction of the data processing operations or their components with other components, data processing operations or services. This includes consideration of any interfaces with sub-processors.
(3) In order to determine conformity with the certification criteria of the AUDITOR Criteria Catalogue, different objects of determination can be assessed. A cloud service is composed of one or more data processing operations. A data processing operation can comprise determination objects, including legally binding agreements (4), processes (5), provider characteristics (6), service characteristics (7), infrastructure components (8), software architecture (9), the development environment (10), personnel of the cloud provider (11) and the (data protection) management system (12).
(4) If legally binding agreements are the object of determination, the characteristics and contents of contracts or agreements with cloud users or subcontracted processors are assessed.
(5) A process or appropriate, accurate process documentation may be reviewed to confirm conformity with the certification criteria.
(6) An examination of provider characteristics includes the assessment of characteristics and features of the cloud provider, such as the underlying organisational structure.
(7) Service characteristics include, in particular, cloud service features and functions that are directly visible to the cloud user and must be verified.
(8) An attestation may include infrastructure components which are physical objects such as hardware components or the data center infrastructure.
(9) The testing of software architecture and its components includes virtual objects, such as source code, as well as the composition and interactions of the individual components of the data processing operations.
(10) Testing of the development environment includes development methods used, a secure test and development environment separate from the production system, and acceptance tests.
(11) An assessment of cloud provider's employees may be necessary, for example, to ensure their professional or personal suitability.
(12) The audit of the (data protection) management system is necessary to identify whether the cloud provider has implemented a system for managing the relevant aspects of its activities, products and services that is in line with the organisation's policy and the certification criteria.

§ 5.2.4 Determination methods

(1) The determination activities must be conducted impartially and structured and managed in such a way as to ensure impartiality (see ISO/IEC 17065:2012 subs 4.2). The evaluators must not allow commercial, financial, or other pressures to compromise impartiality.

(2) Depending on the certification criterion, the determination activities (commonly known as "stage 2 auditing") include a review of documentation provided by the cloud provider (3), inspections (4), tests (5), audits (6), and/or development and design reviews (7).

(3) *Document review* (in the sense of ISO/IEC 17020). In the document review, the evaluator verifies compliance with the certification criteria based on the information in the cloud provider's documentation. A cloud provider submits relevant documents, (technical) logs, certificates and other documentation. A legal analysis takes place (e.g. of the legally binding agreements) to ensure that the applicable legal criteria are met. In addition, certificates of persons (in the sense of ISO/IEC 17024) for proof of competence of the personnel or an individual (e.g. the data protection officer) and to ensure an appropriate level of data protection can be assessed within the scope of a document review. A document review must always be supplemented by appropriate determination methods to ensure that the documented instructions, procedures, rules, etc. are also implemented consistently by the cloud provider.

(4) *Inspection* (in the sense of ISO/IEC 17020). An inspection examines the conformity of a product or process with specific requirements (in this case the GDPR and the certification criteria). Inspection parameters include questions about the quantity, quality, safety, suitability and continued compliance with security of equipment or systems in operation. For AUDITOR certification, compliance with appropriate technical and organisational measures pursuant to Art. 32 (1) lit. a to d GDPR is examined by means of a (legal) inspection. The inspection may include all phases within the scope of the life cycle of the objects of determination, including the development phase. During the inspection, data processing operations can be carried out in the context of service use, for example, in order to assess the functioning and results of the operations. An evaluator compares the expected results according to the available documentation with the actual results produced by use in service. Thus, the evaluator has no insight into the internal processing steps of the processing operations ('black box test'). In addition, a process or a series of processes can also be initiated and the actual execution monitored ('monitoring') or logs of the process execution checked ('white box test').

(5) *Testing* (as defined in ISO/IEC 17025:2017). A test involves means and measurements to examine the data processing operation or the certification object and to determine their compliance with the certification criteria. For example, an asset test may be conducted by examining an asset (e.g. hardware or software code and associated documentation, if applicable). The test may be conducted on the premises of the cloud provider, under the instruction of one of its employees or independently by the evaluator. The cloud provider must be informed in advance of the test and provides the evaluator with, for example, necessary access (e.g. test accounts) or (technical) logs about execution of the process to perform the test. If necessary, the evaluator selects suitable test data. This includes randomly generated values which allow realistic and functionally compliant testing of operation. An evaluator may use appropriate testing products and services (provided externally where appropriate) to test and monitor the process (see ISO/IEC 17025:2017 subs 6.6). The testing products and services used must be documented in the determination report. In the case of invasive test procedures or procedures that could lead to an impairment of data processing operations of the cloud service, coordination with the cloud provider is essential. The cloud provider is obliged to support the evaluator in implementation of the test. For AUDITOR certification, compliance with suitable technical and organisational measures pursuant to Art. 32 (1) a) to d) GDPR is checked by means of a (legal) test. For example, security tests can be used to determine correct and effective encryption of data. When conducting security tests, please refer to ISO/IEC 15408:2009 and ISO/IEC 18045:2008-018.

(6) *Audit* (as defined in ISO/IEC 17021-1:2015). An audit is performed for the purpose of certifying the cloud provider's (data protection) management system (see ISO/IEC 17021-1:2015 subs 3.4) in order to verify that the cloud provider uses a system for managing the relevant aspects of its activities, products and services that is in accordance with the organisation's policy and the certification criteria. Audits may be conducted on-site, remotely or using a combination of the two (see ISO 19011:2018-10 subs 5.5.3). Use of these methods should be appropriately balanced, among other things by considering the risks and opportunities involved. In particular, interviews, observations and exams may be conducted as part of the audit to determine information about knowledge and skills and the extent to which processes and the management system are actually put into practice by the cloud provider. Interviews with employees

of the cloud provider or other persons involved in the provision of the data processing operations can be used to determine the facts about specific aspects and to check the correctness of the documentation (see ISO/IEC 17021-1:2015 subs. B.4). Interviews should be used in particular to check aspects identified as critical by the evaluator. Interviews can be conducted in writing or in person. They are conducted as oral interviews regarding central aspects. If an on-site interview would be disproportionate, it can be conducted in the form of video conferences. Observing a person performing a task can provide direct evidence of competence through the application of knowledge and skills thus demonstrated to achieve a desired outcome (see ISO/IEC 17021-1:2015 subs B.5). Written, oral and practical examinations can provide good and well-documented evidence of existing knowledge and skills, depending on the methodology used (see ISO/IEC 17021-1:2015 subs B.6). An on-site audit includes an inspection of the procedures and technical equipment on the premises of the cloud provider. In the context of the AUDITOR certification, (legal) audits are carried out to verify the correct establishment, maintenance and upkeep of a data protection management system (within the meaning of Art. 24 and 25, 32, 33, 34 and 37 to 39 GDPR). The establishment of a data protection management system should ensure a constant level of data protection for the certified cloud service. For further literature on carrying out audits, please refer to ISO/IEC 17021-1:2015 subs. 9.4 and ISO 19011:2018-10. For remote audits, please refer to IAF MD 4:2018.

(7) *Development and design review* (in the sense of ISO/IEC 17020). A development review includes the review of development methods and procedures and, if required, a review of the test systems and environments used in the development of hardware and software to deliver the data processing operations. The design review may include review of the selected architecture, database diagrams, data flow diagrams, design decisions, but also the configuration of the cloud service to provide the data processing operations. A development and design review should also include a legal analysis to ensure that the applicable legal criteria are met. A legal design and development review may be required as part of the compliance review under Article 25 GDPR or as part of the review of the data protection impact assessment.

(8) The determination methods to be used are specified in the accompanying document *'AUDITOR Investigation Methods'* for each certification criterion and must be applied accordingly by the evaluators.

(9) Determination methods can be combined, if necessary, to gather (additional) well-founded information about the subject of the determination.

(10) The determination may be made on a sample basis in accordance with § 5.2.5.

(11) The determination methods must take account of the relevant international standards. The relevant international standards are ISO/IEC 17025 for testing, ISO/IEC 17020 for inspection, ISO/IEC 17021 for audits of management systems and ISO/IEC 17024 for certification of persons. Reference should also be made to the *"Information sheet on accreditation procedures in data protection"*[2].

(12) An evaluator must ensure that not only sufficient documentation is available as evidence, but also that the documented measures are implemented and put into practice on an ongoing basis by the cloud provider and its personnel. A continuous legal analysis should be carried out during determination activities. For example, evaluators not only review the agreements, but also their concrete implementation by the cloud provider as a processor by means of suitable additional determination methods to ensure that the applicable legal criteria are fulfilled.

(13) The certification body must establish a procedure to ensure integrity and reliability of the collected information during determination activities. In particular, the certification body has to document how the integrity of information supplied by the provider itself can be ensured through concrete verification or other controls by the certification body.

(14) The performance of individual determination activities must be recorded. The records include the date and identity of the persons responsible for each determination activity. Observations, data and calculations are recorded at the time they are made and attributed to the specific determination activity. Changes to the records of earlier versions or to original observations should be traceable.

(15) Determination results and certification-related records must be protected against unauthorised access and protected against manipulation and loss.

§ 5.2.5 Choice of samples during determination activities

[2] https://www.dakks.de/files/Dokumentensuche/Dateien/M%20Informationssicherheits-Managementsysteme_Datenschutz_20211025_v1.1.pdf

(1) A certification body may conduct a sampling when it is neither practical nor cost-effective to review all available information holistically during a determination. For example, records may be too numerous to justify checking every element of the population.
(2) As a rule, a sampling includes the following steps:

(a) Determination of the objectives and reasons for the sampling;
(b) Establishment of the population to be sampled;
(c) Selection of a sampling method (e.g. decision-based or statistical sampling);
(d) Determination of the size of the sample to be taken;
(e) Completion of the sampling activity;
(f) Compilation, assessment, reporting and documentation of the results.

(3) The sample must be selected at least sufficiently broadly, that a representative sampling can be drawn in respect to the population.
(4) When sampling all objects of determination can be involved (s. § 5.2.3), insofar as these could be affected by the certification criteria.
Decision-based sampling or statistical sampling can be applied.
Decision-based sampling relies on the competence and experience of the evaluators to determine samples.
(5) Statistical sampling methods use a sample selection procedure based on probability theory. The evaluators must keep records of sampling that is part of the determination activities. These records must include, where applicable, the following:

(a) a reference to the sampling procedure applied and any sampling criteria used for the assessment (e.g. what is an acceptable sample);
(b) the date when the sample was taken;
(c) a justification for sampling;
(d) the object of determination for which a sample is taken;
(e) description of the population;
(f) data identifying and describing the sample (e.g. size, number, quantity, name);
(g) a designation of the personnel taking samples;
(h) information on the software or hardware used for sampling (if used);
(i) if applicable, the statistical parameters used;
(j) the result of the sample collection.

(6) Reference is made especially to ISO 19011:2018 when sampling during auditing.

§ 5.2.6 Determination with several locations

(1) In situations where the cloud provider performs a data processing operation at multiple locations, such locations must be included in the determination plan (see IAF MD 5:2015 subs 9.1).
(2) The certification body must have documented procedures for carrying out multi-site determination activities (see IAF MD 1:2018 subs 7). These procedures state how the certification body ensures that a data processing operation is performed at all sites and that the operation meets the certification criteria at all sites.
(3) The multi-site determination procedures carried out should be documented and assessed for effectiveness (including principles and procedures for determination) (see IAF MD 5:2015 subs 9.4).
(4) The certification body requires the cloud provider to identify a central site (not necessarily the head office of the organisation) where processes/activities/systems relevant to the provision of the data processing operation are planned, performed or operated and controlled (key activities) and, as appropriate, a number of secondary sites (permanent, temporary or virtual) where similar or additional processes/activities/systems are fully or partially performed (see IAF MD 1:2018 subs 2.4, 5.2, 5.6).
(5) Locations must be fully included in the determination if key activities of the cloud provider are carried out at them (e.g. operation of the computing infrastructure, insofar as the cloud provider is responsible for this). Thus, the central site must be assessed as a minimum.
(6) Sampling from secondary sites is permitted, especially if those sites perform very similar processes/activities (see IAF MD 1:2018 subs 4.6, 6.1.1.1). However, sampling must result in a representative selection of the different sites and ensure that all criteria included in the scope of certification are verified (see IAF MD 1:2018 subs 6.1.2.1).
(7) When determining the size of the sample, the certification body must consider the following (see IAF MD 1:2018 subs 6.1.3):

(a) The certification body must have a documented procedure for determining the size of the sample.
(b) The certification body must document each sampling procedure carried out.
(c) The minimum number of sites to be assessed per determination is:
    (i) Initial test: the size of the sample must be the square root of the number of secondary sites: ($y=\sqrt{x}$), rounded to the higher integer, where y = the number of secondary sites to be included in the sample and x = the total number of secondary sites.
    (ii) Surveillance test: the size of the annual sample must be the square root of the number of sites multiplied by the factor of 0.6 as a coefficient ($y=0.6*\sqrt{x}$), rounded up to the nearest integer.
(d) The central site must be assessed during each initial certification and at least once a year as part of the surveillance.
(e) At least 25% of the samples must be selected randomly (see IAF MD 1:2018 subs 6.1.2.2). The remainder are selected in such a way that the differences between the sites selected over the certification validity period are as large as possible (see IAF MD 1:2018 subs 6.1.2.3). In addition, each site must be inspected at least once during the certification validity period.
(f) The size or frequency of the sample is increased if the risk analysis of the certification body for the data processing operation or the secondary sites reveals special circumstances (e.g. changes in the location, results of internal audits of the cloud provider, changes in risks).
(g) If the structure of the cloud provider changes (e.g. addition of a new site), the certification body will adjust the sampling procedures. This includes considering whether to assess the new site(s).

Example:
- 1 central site (head office): Inspection at each determination cycle (initial assessment and surveillance)
- 4 national branches: Sample = 2: at least 1 at random
- 27 regional offices: Sample = 6: at least 2 at random

(8) Certification bodies must have documented procedures to restrict sampling procedures where they are not appropriate to provide sufficient confidence (see IAF MD 1:2018 subs 6.1.1.4, 6.1.2.4, IAF MD 5:2015 subs 9.2, 10.3). Such limitations may be imposed by the certification body in relation to the following factors:

(a) the risks to a data processing operation for a site;
(b) total number of personnel at the site;
(c) significant differences in the size of the sites;
(d) complexity of the activities at the site;
(e) deviations in the business purpose of the sites;
(f) deviations in working procedures or the activities carried out;
(g) complexity of the information systems at the various sites;
(h) possible interactions with critical information systems;
(i) existence of several/separate data protection management systems per site;
(j) variations in the design and operation of the controls;
(k) records of complaints and other relevant aspects for corrective and preventative measures;
(l) data and information security incidents at the individual sites;
(m) results of internal audits at the sites and management assessments or previous certifications;
(n) deviating legal requirements;
(o) differences in culture or language;
(p) geographical location distribution;
(q) permanent or temporary nature of sites.

(9) If the certification body determines that a sample-based procedure cannot be applied, an individual assessment of the sites is required (see IAF MD 1:2018 subs 1, 4.6, 6.2):

(a) the determination plan must include an initial assessment for all sites;

(b) for surveillance activities, 30% of all sites, rounded to the nearest whole number, must be assessed annually;
(c) each determination must include the central site;
(d) the sites selected for the second surveillance procedure will usually be different from those selected for the first.

(10) Typically, on-site assessments would be carried out at secondary sites. However, the following procedures should be considered as possible alternatives to replace some on-site assessments (see IAF MD 5:2015 subs 9.3):

(a) face-to-face interviews or meetings or conference calls with the cloud provider;
(b) verification of activities at secondary sites on the basis of documents;
(c) remote retrieval of electronic sites containing records or other information relevant to the data processing operation and the secondary site(s) being assessed;
(d) use of video and telephone conferencing and other technologies that enable effective remote investigation.

§ 5.2.7 Determination activities in the case of third country transfers of data

(1) Insofar as a third country data transfer cannot be excluded within the scope of the certification object, the certification body must check whether the relevant criteria for the third country transfer are met. Special attention should therefore be paid to the determination activities of the criteria under Nos. 1.4, 3 and 11 in the AUDITOR Criteria Catalogue.
(2) In the case of a third country transfer, evaluators must therefore determine and document (1) whether the cloud provider complies with its obligations under Article 28 GDPR, in particular whether the transfer in question is covered by instructions from the data controller, and (2) the extent to which the specific requirements under criteria catalogue No. 11 are followed (see DSK ADZ subs. 2.10).

§ 5.2.8 Determination report

(1) The evaluators produce a determination report based on the determination activities, presenting the results of the determination accurately, clearly, unambiguously and objectively (see ISO/IEC 17065:2012 subs 7.4.9, DSK subs 7.4).
(2) In general, the determination report must reflect the two assessed levels of the cloud provider: first, the data protection management system of the cloud provider as an organisation, and second, fulfilment of the certification criteria in relation to the data processing operation to be certified.
(3) The determination report must contain at least the following information:

(a) clear headings, so that all parts of the determination report can be identified as part of a complete report, and a clear indication of the end of the report;
(b) the date of issue of the report;
(c) details of the evaluators who carried out the determination process, including the name and company address;
(d) details of the cloud provider, including the name and address;
(e) a detailed description of the object of certification, indicating all relevant data processing operations, so that a closed structure is ensured (see § 5.1.4);
(f) a representation of the chronological sequence, including at least the start and end dates of the determination;
(g) a description of the scope of the determination, indicating the locations and premises at which the determination was conducted, including if conducted at the cloud provider's premises or at locations other than the evaluators' or certification body's permanent premises or associated temporary or mobile premises;
(h) the measures used by the evaluators for determination, in particular information on methods of determination according to § 5.2.4 and, if necessary for understanding, a justification of their use;
(i) a list of the determination objects assessed (see § 5.2.3);
(j) information on the use of technical testing software and hardware (e.g. programs used to conduct technical assessments);
(k) an indication of the certificates recognised by the certification body and the results of the sample verification;
(l) a statement on verification of the interaction between the data processing operations;

(m) if applicable, information on special determination conditions, such as environmental conditions;
(n) if applicable, the determination inaccuracies that can occur or risks that exist in relation to determination accuracy, repeatability and reproducibility (see ISO/IEC 17007 subs. 5.4.1);
(o) a description of the implementation of the data protection management system;
(p) a description of the implementation of the individual certification criteria. The level of detail of the description must at least be comprehensive enough to include all necessary information to enable a clear assessment of conformity with the individual certification criterion without doubt and without uncertainties;
(q) if required, a statement of conformity for each of the certification criteria. Evaluators must present the statement of conformity in such a way that the results to which the statement of conformity applies are clear, which certification criteria are met or not met by an object of determination and which decision-making rule was applied. Opinions and interpretations of statements from determination activities must be clearly distinguished from statements about conformity;
(r) a declaration by an evaluator that he/she has fulfilled the certification requirements of this conformity assessment scheme regarding independence and impartiality and that there is no bias.

(4) The complete determination report must be made available during the accreditation procedure and at any time at the request of the data protection supervisory authority (see EDPB Annex 1 subs. 7.4).
(5) Evaluators must take responsibility for all information provided in the report, unless the information is provided by the cloud provider or a third party. Data provided by a cloud provider, or third party must be clearly identified as such. In addition, the report must include a statement if the information is provided by the cloud provider or a third party and may impact the validity of the findings.
(6) The evaluators make the determination report available electronically or as a hard copy to the certification body and the cloud provider and grant them unrestricted rights of use. The cloud provider may only make the determination report available to third parties in full, with an indication of the date of issue, and may impose appropriate restrictions on use by such third parties. The certification body may reserve the right of publication and public reproduction within the meaning of Section 15(2) UrhG.
(7) If a report that has been issued needs to be amended or reissued, any changes to the information must be clearly identified and, where necessary, the reason for the change must be included in the report. Amendments to a report after it has been issued may only be made in the form of a separate document or data transmission in which the words "Amendment to report, document ID ... [or other identification]" or equivalent wording appear. If it is necessary to issue a completely new report, this report must have a unique designation and contain a reference to the original which it replaces.

5.3 Review

§ 5.3.1 Review of the results of the determination activities

(1) The decision-makers assess the fulfilment of the certification criteria of the AUDITOR Criteria Catalogue by the data processing operations in relation to a specific protection category and restorability class based on the findings from the evaluation (i.e. selection and determination activities). This requires a review of the fulfilment of each individual certification criteria and of overall fulfilment of the entire certification criteria of the AUDITOR Criteria Catalogue, each in relation to a specific protection category and restorability class.
(2) The review must be carried out by personnel of the certification body (decision-makers) who have not been involved in determination activities in order to prevent possible conflicts of interest and ensure impartiality (see ISO/IEC 17065:2012 subs. 7.5.1, DSK subs. 7.5). The certification body must demonstrate that the person(s) responsible for the review were not directly or indirectly involved in the determination activities. The implementation of these requirements and their results must be documented as part of the review (see DSK subs. 7.5).
(3) Recommendations for a certification decision based on the review must be documented unless the review and certification decision are made simultaneously by the same person (see ISO/IEC 17065:2012 subs. 7.5.2). The certification body must report its decision in such a way that it is clear to which results the statement of conformity applies, which certification criteria are met or not met by a certification object, and which decision-making rule was applied.

(4) The certification body may collect additional information and evidence from the cloud provider to the extent necessary for the review.
(5) If individual certification criteria of the AUDITOR Criteria Catalogue are not applicable to the respective certification object (see § 5.1.5), this must be indicated and justified separately within the framework of the justification of the overall result.
(6) The review results in a recommendation for the certification decision.

§ 5.3.2 Non-conformities with certification criteria

(1) The decision-maker reviews conformity with the certification criteria. For this purpose, the conformity of each individual subsection of a certification criterion must be assessed. The following review standard must be applied to each subsection of a certification criterion:

- (a) Fulfilment (compliance)
  - (i) number of the certification criterion is fulfilled.
- (b) fulfilment (compliance) with recommendation
  - (i) deviation the significance of which does not call into question compliance with the data protection requirements as a whole (potential for improvement).
  - (ii) examples:
    1. The encryption method used is still "state of the art", but should be replaced in the near future.
    2. As no password policy is specified regarding password reuse, employees can reuse an original password.
    3. The IT security manual should be updated and follow a standardised methodology.
- (c) non-conformity
  - (i) Significant deviation, with the result that there is considerable doubt that the data protection requirements are fundamentally met.
  - (ii) Examples:
    1. The required documentation (e.g. process documentation, functional documentation or logs) cannot be provided by the cloud provider or performance of data processing operations to verify compliance with criteria is not possible.
    2. Process documentation is available, but the process is not put into practice consistently during cloud service operation.
    3. Security tests have revealed serious deficiencies or vulnerabilities in the cloud service software used.
    4. Survey or on-site inspection as part of an audit has revealed a failure to implement certification criteria.

(2) If a subsection of a criterion is deemed to be a "non- conformity ", the criterion as a whole is also considered not to have been met.
(3) Non-conformities must be rectified before certification is granted.
(4) If the review has determined that one or more certification criteria are not fulfilled, the certification body checks whether a revision can be implemented successfully by the cloud provider within a reasonable period of time (see ISO/IEC 17065:2012 subs. 7.4.7). The deadline can be extended at the request of the cloud provider.
(5) The certification body must clearly describe to the cloud provider any deficiencies or deviations that prevent compliance with the certification criteria (see ISO/IEC 17065:2012 subs 7.4.6, EDPB Annex 1 subs 7.4). The certification body must help to clarify any ambiguities in the event of queries, provided that this support does not compromise impartiality.
(6) The certification body requires the cloud provider to analyse the root causes and describe the specific corrective measures taken or planned to address the identified non-conformities within a specified time period.
(7) Within the scope of the revision, the cloud provider must ensure that all deficiencies and deviations in relation to fulfilment of the certification criteria are remedied.
(8) After completion of the revision, the cloud provider must provide the certification body with all necessary documents to demonstrate that the revision has been successful.
(9) The certification body evaluates the corrections and corrective measures submitted by the cloud provider to determine whether they are acceptable (see ISO/IEC 17065:2012 subs. 7.4.7, 7.4.8). The certification body verifies the effectiveness of all corrections and corrective measures taken. The evidence obtained of revision of the non-conformities must be recorded. The cloud provider is informed of the outcome of the review and verification.

(10) Depending on the extent and severity of the required revision, the certification body may schedule a re-assessment within a reasonable period of time. During this re-assessment, the certification requirements of determination apply and corresponding determination activities according to § 5.2.4 are applied on a sample basis, if necessary.
(11) If it was determined during the evaluation of the corrections or the re-assessment that one or more certification criteria are still not fulfilled, the certification body considers whether a further revision can be carried out successfully by the cloud provider within a reasonable period of time and appears appropriate. The period may be extended at the request of the cloud provider.
(12) As part of the surveillance, the certification body must check whether the recommendations have been complied with. If not, the certification body checks whether the previous recommendation has become a non-conformity due to changes in conditions.

§ 5.3.3 Non-conformities of certification criteria at different sites

(1) If non-conformities are found at individual sites, either during the cloud provider's internal audit or during the certification body's determination, it must be assessed whether other sites may also be affected (see IAF MD 1:2018 subs 7.7.1). For this reason, the certification body must require the cloud provider to review their non-conformities to assess whether or not they represent a general deficiency in the cloud service that also applies to other sites.
(2) If this is found to be the case, corrective measures must be taken and assessed, both at central sites and at each of the affected secondary sites (see IAF MD 1:2018 subs 7.7.1).
(3) If it is determined that this is not the case, the cloud provider must be able to demonstrate to the certification body that a limitation of the revision to certain sites is justified (see IAF MD 1:2018 subs 7.7.1).
(4) If, at the time of the decision process, one of the sites has a non-conformity, certification is denied to the entire multi-site organisation until satisfactory corrective measures have been taken (see IAF MD 1:2018 subs 7.7.3, 7.7.4). The cloud provider is not permitted to exclude a "problematic" site during the certification process to overcome the obstacles encountered due to the existence of a non-conformity at a single site.

5.4 Decision on certification

§ 5.4.1 Decision of the certification body

(1) Based on the determination report and the review, the decision-makers decide whether to grant the certification and award the conformity marks.
(2) The period between the completion of the last determination activity and the certification decision may only exceed 3 months in justified exceptional cases (see DSK point 7.3).
(3) The certification decision may only be made by persons appointed by the certification body (decision-makers) who are bound by a contract or formal agreement to (see ISO/IEC 17065:2012 subs. 7.6.3 and 7.6.4):

(a) the certification body;
(b) a unit under organisational control of the certification body.

(4) The certification decision is taken by a person or group of persons (e.g. a committee) who were not involved in the determination activities (see ISO/IEC 17065:2012 subs 7.6.2). The review and decision on certification may be carried out simultaneously by the same person or group of persons.
(5) The decision on certification must be made by the head of the certification body or a qualified person directly appointed by them (see DSK subs. 7.6).
(6) The certification body must explain in detail how its independence and accountability regarding certification decisions are ensured (see DSK subs. 7.6, EDPB Annex 1 subs. 7.6).
(7) The certification body must inform the cloud provider of the reasons for not granting a certification (see ISO/IEC 17065:2012 subs 7.6.6). If the cloud provider expresses interest in continuing the certification process, the certification body may resume the selection and determination processes.

§ 5.4.2 Appeal by the cloud provider

(1) The cloud provider may appeal to the certification body against its decision. Reasons must be given for the appeal.
(2) An appeal is a request by the cloud provider to a certification body to review its decision regarding the certification object (see ISO/IEC 17000:2004 subs 6.4).

(3) The appeal must be submitted in text form within a period of 4 weeks of receipt of the certification decision.
(4) The certification body checks whether the appeal is justified.
(5) If the appeal is directed against the selection or determination activities or the findings of the evaluators, the certification body informs the evaluators about the appeal and obtains a statement from them.
(6) If the appeal is upheld, the certification body must amend the certification decision. If the certification body does not process the appeal, reasons must be given.
(7) The decision on the appeal including the reasons is communicated to the cloud provider in text form.

5.5 Attestation

§ 5.5.1 Granting of certification

(1) Certification is granted by the certification body to the extent requested (i.e. for a specific protection category and restorability class) if the data processing operations meet the certification criteria of the AUDITOR Criteria Catalogue and the certification body has informed the competent data protection supervisory authority of the reasons for granting certification.
(2) The certification body must inform the competent data protection supervisory authority of the certification in writing at least one week before the certification is granted (see DSK subs. 7.6, EDPB Annex 1 subs. 7.8). This notification must include the name of the certification body, a description of the certification object and the public summary report.

§ 5.5.2 Granting of the right to use conformity marks

(1) The granting of certification entitles the cloud provider to bear a quality seal of approval and a certificate as marks of conformity for the certified data processing operations.
(2) The certification body assigns a unique certificate number to each certificate. It is composed of the unique name of the certification body, the indication "AUDITOR" and a number unique within the certification body (example: CERTIFICATION BODY-AUDITOR-0001). The certificate number must be indicated on all marks of conformity for traceability purposes.
(3) A mark of conformity may be used only during the period of validity of the certification and the accreditation of the certification body.
(4) The certification body issues the marks of conformity as follows:

(a) The certificate is provided to the cloud provider by post and electronically.
(b) The quality seal is provided graphically in electronic form.

(5) The certification body must ensure correct use of the mark of conformity for the period of validity (see § 4.4.3).

§ 5.5.3 Content of the quality seal

(1) The quality seal contains the following information:

(a) the graphical conformity mark;
(b) short title, data processing operation and data protection role ("as processor pursuant to Art. 4 No. 8 GDPR");
(c) the certificate number;
(d) the period of validity of the certification with an indication of the period (date of issue, duration);
(e) the designation AUDITOR with protection category 1, 2 or 3;
(f) the indication of the restorability class 1, 2 or 3.

(2) If the quality seal is included in electronic media (e.g. website), this must have a link to the entry in the certification body's certification register (see § 4.4.2) in order to facilitate traceability by cloud users and interested parties.

§ 5.5.4 Contents of the certificate

(1) The certificate contains the following information:

(a) the cloud provider, if applicable as a short name;
(b) address of the cloud provider, secondary locations if applicable;
(c) data protection role according to the GDPR "as a processor pursuant to Art. 4 No. 8 GDPR";

(d) regional scope: Germany, EU, third country;
(e) the certification object, if applicable as a short designation;
(f) the certification body and its address;
(g) the certification statement that the certified data processing operations meet the relevant requirements of the GDPR and the BDSG according to the AUDITOR Criteria Catalogue in its latest version for a specific protection category and a specific restorability class and the additional requirements of the data protection supervisory authorities;
(h) the name of the relevant version of the AUDITOR conformity assessment scheme and criteria catalogue;
(i) a unique certificate number;
(j) date of the certification decision;
(k) indication of last audit date on site: < dd.mm.yyyy> /report number/date;
(l) the period of validity of the certification indicating the period, date of issue of the certificate: "date of issue <dd.mm.yyyy>" and "duration until <dd.mm.yyyy> max. 3 years>";
(m) brief information about surveillance, e.g. "within the validity period the certificate will be monitored annually for compliance"; and “next planned surveillance by < dd.mm.yyyy>”.
(n) confirmation of the notification of the certification decision to the data protection supervisory authority "The reasons for granting the certificate were notified to [data protection supervisory authority XYZ] in accordance with Art. 43(5) GDPR on DD.MM.YYY."
(o) an appendix containing the information referred to in (2); and the references to those appendices "[data processing operation] in accordance with Appendix 1" and "subject to the exclusions of use in accordance with Annex 2".
(p) accreditation symbol;
(q) logo of the certification body, if applicable;
(r) signature of the head of the certification body or representative.

(2) The appendices to the certificate contain the following information:

(a) Appendix 1:
  (i) the unique name of the cloud provider, including address;
  (ii) a detailed description of the certification object;
  (iii) reference to the public summary report of the result of the certification pursuant to points 7.6 and 7.8 of the requirements for accreditation of Art. 43 (3) GDPR in conjunction with DIN EN ISO/IEC 17065 of the DSK. The public summary report must document the use of the certification object in the area of application and the use cases in a transparent and comprehensible manner, so that the (end) customer or a data subject can also comprehend in a reasonable time what is guaranteed when using the certification object in the sense of data protection law;
  (iv) if applicable, the designation of the regulations of the certification body that have been used;
  (v) further instructions from the certification body, if applicable.
(b) Appendix 2:
  (i) This specifies all exclusions of use, for instance what is not guaranteed when using the certification object in the area of application.

(3) Furthermore, reference should be made to the *"Information sheet on accreditation procedures in data protection"*[3], which has a template certificate in its appendix.

§ 5.5.5 Period of validity and preservation of certification

(1) The certification is granted for a period of three years. The period begins with the date of issue shown on the mark of conformity.
(2) The cloud provider can apply for preservation of the certification in the form of an extension of the certification before or after expiry of the validity period. In this case, the certification object is re-certified.
(3) The certification body may issue the renewed certification on the date immediately following the expiry of the validity period of the previous certification if the application is submitted in good time and the certification process has been completed.

[3] https://www.dakks.de/files/Dokumentensuche/Dateien/M%20Informationssicherheits-Managementsysteme_Datenschutz_20211025_v1.1.pdf

(4) If existing certificates of the cloud provider are recognised, the validity period of the AUDITOR certification is reduced to the expiry date of the shortest recognised certificate (see DSK point 7.4). In the case of re-certification of the recognised certification, the expiry date of the AUDITOR certification is extended to the term of the recognised certificate, but at most to the standard term of the AUDITOR certification of 3 years or, in the case of recognition of other third-party certificates, to the shortest term. If no re-certification of the recognised certificate is carried out, at least the area originally covered must be re-examined to maintain the validity of the AUDITOR certification.

§ 5.5.6 Appeal by the data protection supervisory authority

(1) If the certification body is instructed by the data protection supervisory authority to revoke a certification it has granted pursuant to Article 58 (2) (h) GDPR or not to grant a certification, the certification body must ensure that the relevant cloud provider is informed of this and of the consequences of it (see DSK subs. 8.12). Corresponding certification register entries are adjusted and the data protection supervisory authority is informed of this.

§ 5.5.7 Certification documentation

(1) The certification body issues the cloud provider with formal certification documentation that clearly conveys or permits identification of the following elements (see ISO/IEC 17065:2012 subs. 7.7.1, EDPB Annex 1 subs. 7.7):

(a) the name and address of the certification body;
(b) the date on which certification was granted (the date must not be earlier than the date on which the certification decision was taken);
(c) the name and address of the cloud provider;
(d) the scope of the certification, including a precise description of the data processing operations as the object of certification;
(e) the period or expiry date of the certification if the certification expires after a specified date;
(f) the frequency and other information about the surveillance activities required;
(g) information about the application and determination and evaluation reports;
(h) the certification agreement;
(i) a reasoned review of fulfilment, recommendation, non-conformity or non-applicability of the individual certification criteria for the given protection category and restorability class;
(j) the overall result regarding the fulfilment or non-fulfilment of the certification criteria for a specific protection category and restorability class;
(k) a justification of the overall result;
(l) verification of corrections and corrective measures, if applicable;
(m) records of complaints and appeals, if any, and subsequent corrections or corrective measures.

(2) The formal certification documentation includes the signature or other specified authority of the person(s) of the certification body to whom such responsibility is assigned (see ISO/IEC 17065:2012 subs. 7.7.2).
(3) The certification body stores records relating to applicants and certified cloud providers securely to ensure that the information remains confidential (see EDPB Annex 1 subs 7.12). Records must be transported, delivered and transmitted in a confidential manner. Records from certified cloud providers and previous certified cloud providers must be retained for the duration of the current certification cycle plus one additional full certification cycle.
(4) According to ISO/IEC 17065:2012 subs. 7.8, the certification body must publish a public summary of the result of the certification (see DSK subs. 7.6, EDPB Annex 1 subs. 7.8). The certification object (including the version or the functional status), the underlying criteria, the determination methods applied and the results must also be evident in this.

5.6 Surveillance

§ 5.6.1 Carrying out regular surveillance activities

(1) During the period of validity, the data processing operations are subject to surveillance in the form of an interim assessment to be carried out at least annually.
(2) In addition, surveillance activities can be carried out on an ad hoc basis in the event of anomalies that give rise to fears of non-conformity with the certification criteria.

(3) The procedure for surveillance and the corresponding entries in the certification agreement must be provided at any time in the accreditation procedure on request of the data protection supervisory authority.
(4) Based on the interim assessment, the certification body determines whether the certified data processing operations continue to meet the certification criteria according to the specified protection category and restorability class.
(5) The certification body reminds the cloud provider and, as appropriate, (outsourced) evaluators in good time of an upcoming interim assessment and points out the consequence of failing to carry out the interim assessment.
(6) The annual interim assessment must be carried out at the earliest after sixth months and at the latest after twelve months of granting the certification or the corresponding dates in subsequent years.
(7) If the interim assessment is not carried out within the specified period, the certification body takes measures in accordance with § 5.6.4.
(8) The cloud provider is required to participate in surveillance activities.
(9) The requirements of this scheme for selection, determination, review and decision-making activities apply accordingly to the interim assessment (see ISO/IEC 17065:2012 subs. 7.9.2).

§ 5.6.2 Scope of surveillance activities

(1) The scope of the interim assessment is such that, as a minimum, the changes in the data processing operations that have occurred since the last assessment are examined by applying determination methods (see § 5.2.4). Appropriate sampling (see § 5.2.5) is used to determine whether the data processing operations continue to meet the certification criteria (see ISO/IEC 17000:2004 subs. A.5.4).
(2) As part of the surveillance, the certification body checks that recognised certificates are still valid. If a certification body determines that a recognised certificate is no longer valid and the cloud provider has not informed the certification body in advance and arranged for appropriate measures in consultation with it (e.g. a re-certification with a different scope), the certification body takes appropriate measures in accordance with § 5.6.4.
(3) The total time spent annually on surveillance activities should be approximately one third of the determination time spent on the initial certification (see IAF MD 5:2015 subs 5). The planned surveillance time should be reviewed from time to time to consider changes that affect it.
(4) Continuous certification may be carried out to verify compliance with the certification criteria at all times (see Lins et al. (2016)). For continuous certification, test and monitoring-based procedures can be used which collect data demonstrating conformity with the certification criteria (see Lins et al. (2019)). The testing frequency depends on the certification criterion to be tested.

§ 5.6.3 Review of the surveillance activities

(1) The evaluators prepare an interim assessment report and submit it to the certification body in advance before the end of the interim assessment period.
(2) The decision-makers review the interim assessment report and decide without delay on the preservation, restriction, suspension or withdrawal of the certification (see § 5.6.4)
(3) Where non-conformity with certification criteria is revealed, either because of surveillance activities or otherwise, the certification body considers and decides on appropriate measures in accordance with § 5.6.4 (see ISO/IEC 17065:2012 subs 7.11.1).

§ 5.6.4 Determination of non-conformity with certification criteria

(1) The cloud provider is obliged to inform the certification body in detail and without delay if it becomes aware that the prerequisites for granting certification did not exist or no longer exist (e.g. withdrawal of recognised certificates).
(2) If, based on surveillance activities, communications from the cloud provider or a third party, or other circumstances, the certification body has reason to believe that the prerequisites for granting certification did not exist or no longer exist (see also § 5.3.2 and § 5.3.3), the certification body immediately takes the necessary measures to assess this situation (see ISO/IEC 17065:2012 subs.7.11.1). In addition, the certification body may take the following measures:

    (a) the certification body may in particular determine that an interim assessment is necessary to maintain certification;

(b) the certification body may recommend re-certification with a different scope to the cloud provider (see § 5.6.9);
(c) the certification body may allow the continuation of certification under conditions set by the certification body (e.g. increased surveillance), provided that the non-conformity of certification criteria does not compromise the requirements of the certified protection category and immediate remedial measures are taken by the cloud provider.

(3) The certification body must clearly describe to the cloud provider the aspects which give rise to doubts about compliance with the certification criteria (see EDPB Annex 1 subs. 7.4).
(4) If the certification body determines that an interim assessment is necessary, the following requirements must be met:

(a) the certification body sets the cloud provider a reasonable deadline for carrying out the interim assessment. The deadline may be extended at the request of the cloud provider;
(b) an interim assessment must meet the requirements of selection, determination, review and decision-making activities of this scheme (see ISO/IEC 17065:2012 subs 7.11.2, subs 7.11.5);
(c) if selection and determination activities are necessary for an interim assessment, these may be carried out by (outsourced) evaluators;
(d) necessary review and decision-making activities are carried out by the certification body. The certification body must appoint personnel for this purpose who have the necessary competences, as described under § 4.2.3 (see ISO/IEC 17065:2012 subs. 7.11.4).

(5) Based on the review, the certification body takes the measures necessary to establish compliance with the AUDITOR catalogue of criteria. These include:

(a) the certification body may restrict the certification (see § 5.6.5);
(b) the certification body may suspend certification for a specified period of time subject to the cloud provider taking remedial measures (see § 5.6.6);
(c) the certification body may revoke the certification (see § 5.6.7).

(6) The certification body must give the cloud provider the opportunity to comment before making its decision. The decision must be justified and sent to the cloud provider in text form.
(7) Re-certification with a different scope may be carried out at the request of the cloud provider.

§ 5.6.5 Restriction of certification

(1) Even though the certification criteria for the protection category applied for are not met, certification may be granted with limitations or may be restricted, instead of withdrawal or suspension, if the certification criteria for a lower protection category are met. In such cases, a certification may be granted for a lower protection category.
(2) The cloud provider may request restriction of certification at any time. The application must be granted unless there are good grounds for not doing so.
(3) The restriction of certification takes effect three weeks after notification of the decision on the restriction.
(4) If a certification is restricted, the certification body must act and make any necessary changes to formal certification documents, public information and permission to use marks of conformity, etc. to ensure that the restricted scope of certification is clearly communicated to the cloud provider and clearly described in the certification documentation and public information (see ISO/IEC 17065:2012 subs. 7.11.3). This includes changing the mark of conformity and the entry of the data processing operations in the register of certified data processing operations.
(5) The certification body must ensure that the cloud provider modifies its advertising with the certification in accordance with the restriction and implements other measures defined by the certification body.
(6) The supervisory authority must be informed of the restriction (see EDPB Annex 1 subs. 7.11).
(7) The certification body requests the cloud provider to inform its cloud users about the restriction.

§ 5.6.6 Suspension of certification

(1) Suspension means a temporary suspension of the statement of conformity for all or part of the specified scope of the certification (see ISO/IEC 17000:2004 subs. 6.2).
(2) The cloud provider may request the suspension of the certification at any time. The application must be granted unless there are good reasons for not doing so.
(3) The certification body may suspend certification for the duration of a determination.

(4) The suspension takes effect immediately.
(5) If a certification is suspended, the certification body must take steps to make any necessary changes to formal certification documents, public information, permits to use marks, etc. to ensure that they do not give any suggestion that the data processing operations are still certified (see ISO/IEC 17065:2012 subs 7.11.3). This includes withdrawal of the mark of conformity and removal of the data processing operations from the list of certified data processing operations.
(6) The certification body ensures that the cloud provider stops advertising with the certification and implements further measures defined by the certification body.
(7) When certification is re-instated after suspension, the certification body makes any necessary changes to formal certification documents, public information and permission to use marks, etc. to ensure that all appropriate indications that the data processing operations are still certified are in place (see ISO/IEC 17065:2012 subs 7.11.6). The cloud provider may then also continue to advertise the certification.
(8) The data protection supervisory authority must be informed of the suspension (see EDPB Appendix 1 subs. 7.11).
(9) The certification body requests the cloud provider to inform its cloud users about the suspension.

§ 5.6.7 Withdrawal of certification

(1) Withdrawal means the revocation of certification (see ISO/IEC 17000:2004 subs 6.3).
(2) The cloud provider may request withdrawal of the certification at any time. The application must be granted unless there are good reasons for not doing so.
(3) The certification is withdrawn if

(a) the certification body concludes that the conditions for granting certification were not met or are no longer met;
(b) the data protection supervisory authority responsible for the cloud provider determines that the requirements for certification were not met or are no longer met (see EDPB Annex 1 point 7.11). Withdrawal is carried out by the certification body on the instruction of the competent data protection supervisory authority (Art. 58 (2) (h) GDPR);
(c) if an interim assessment is not carried out or not carried out within the specified period;
(d) if the accreditation of the certification body is suspended or withdrawn (see § 4.1.1);
(e) if the AUDITOR scheme owner determines that the AUDITOR Criteria Catalogue does not or no longer fulfils the legal requirements of the General Data Protection Regulation and the BDSG, or the legal provisions replacing them. This does not apply if the cloud provider immediately applies for re-certification with a different scope according to a new version of the AUDITOR Criteria Catalogue and this is carried out without delay.

(4) The withdrawal takes effect three weeks after the decision on the withdrawal has been issued.
(5) If a certification is withdrawn, the certification body takes steps to make any necessary changes to formal certification documents, public information, permits to use marks, etc. to ensure that they do not give any indication that the data processing operation is still certified (see ISO/IEC 17065:2012 subs 7.11.3). This includes in particular the withdrawal of the mark of conformity as well as the removal of the data processing operation from the list of certified data processing operations.
(6) The certification body ensures that the cloud provider stops advertising with the certification and implements further measures defined by the certification body.
(7) The supervisory authority must be informed of the withdrawal (see EDPB Annex 1 subs. 7.8).
(8) The certification body requests the cloud provider to inform its cloud users of the withdrawal.

§ 5.6.8 Extension of the certification

(1) The cloud provider can apply for an extension of the certification at any time. The extension relates to an increase in the protection category and / or restorability class.
(2) The cloud provider must prove that it meets the requirements of the higher protection category and / or restorability class as part of re-certification with a different scope.
(3) The certification body evaluates the results of the re-certification with a different scope and decides on the award of a certification with a higher protection category and / or restorability class.
(4) The requirements for selection, determination, review and decision-making activities also apply in case of an extension.

§ 5.6.9 Re-certification with a different scope

(1) If this conformity assessment scheme or the AUDITOR Criteria Catalogue introduces new or revised certification criteria or other requirements that affect the cloud provider, the certification body must ensure that these changes are brought to the attention of all cloud providers (see also § 4.3.5) (see ISO/IEC 17065:2012 subs 7.10.1).

(2) The certification body must set a reasonable deadline for the implementation of the criteria or requirements for a cloud provider and inform the cloud provider of it. The deadline may be extended at the request of the cloud provider.

(3) The certification body verifies the implementation of the changes by the cloud providers. In particular, the certification body may determine that an interim assessment is required to maintain certification.

(4) If the certification body determines that an interim assessment is necessary, it must set the cloud provider an appropriate deadline for carrying out the interim assessment. The certification body must describe clearly to the cloud provider the aspects which give rise to doubts about compliance with the certification requirements. The deadline may be extended at the request of the cloud provider.

(5) The certification body may suspend certification for the duration of the re-certification with a different scope (see § 5.6.6).

(6) The certification body takes the measures necessary to ensure compliance with the AUDITOR Criteria Catalogue based on its findings. It may decide to declare the certification still valid, or restrict, suspend or withdraw it. The certification body gives the cloud provider the opportunity to comment before making its decision. The decision is justified and sent to the cloud provider in text form.

(7) The certification body considers other changes that may affect certification, including changes triggered by the cloud provider, and decides on the appropriate measures (see ISO/IEC 17065:2012 subs. 7.10.2). These include in particular:

   (a) changes to certified data processing operations of the cloud provider in accordance with § 4.3.3;
   (b) changes in the regulatory and IT environment of cloud services, including, for example, identification of new security vulnerabilities and weaknesses or developments in the state of the art (see also § 4.3.5and § 4.3.4);
   (c) a decision that previous security measures are considered insufficient or insecure, such as the use of outdated encryption methods.

6 Appendix A: Definition and calculation of the determination time

6.1 General

6.1.1 Basics

The certification body must have documented procedures for calculating the time required for determination activities (see ISO/IEC 17065:2013 subs. 7.4.1). For each cloud provider, the time required to plan and conduct a complete and effective determination is calculated individually. In principle, the determination time must be short in order to enable certification of small and medium-sized cloud providers (as defined in Art. 42 (1) GDPR). At the same time, the widest possible scope of determination and sufficient depth of determination must be achieved to uphold the protection statement of the AUDITOR certification and compliance with the requirements of the General Data Protection Regulation. Basic concepts for calculating the amount of work involved in the determination process are specified below, as an example of the amount of time and effort involved in determination and an aid to achieving budgetary planning reliability for cloud providers and certification bodies.

6.1.2 Distribution of determination time

The determination time includes the on-site time on the cloud provider's premises as well as the time spent off-site in conducting the planning and document review, communicating with the cloud provider's personnel and writing the determination report (see IAF MD 5:2015 subs 2.1). A determination day usually comprises 8 hours. Travel (to, from or between locations) and any interruption are not included in the determination time. The time spent by team members who are not assigned as evaluators (e.g. subject experts, translators, interpreters, observers and auditors-in-training) does not count towards the specified determination time.

The planned determination time should be divided into the aspects "project overhead and document review", comprising approx. 35% (this includes, for example, time spent planning and reporting), and "detailed determination", comprising approx. 65% of the total work. Detailed determinations mainly involve on-site determination activities. If remote techniques such as web meetings, telephone conferences and remote electronic testing of data processing operations (e.g. penetration tests or vulnerability assessments) are used, these activities should be listed in the determination plan (see § 5.2.2) and can be considered as part of the overall "detailed determination". However, remote testing may only account for more than 30% of the planned on-site determination time in exceptional cases. If additional time is required for planning and/or preparation of reports, this is not a justification for reducing the on-site determination time.

The total time spent annually on surveillance should be approximately one third of the determination time spent on the initial certification (see IAF MD 5:2015 subs 5, and § 5.6.2). The planned surveillance time should be reviewed from time to time to consider changes that affect it.

To ensure the effectiveness of the determination, the certification body should also consider the composition and size of the determination team (e.g. ½ day with 2 evaluators may be less effective than 1 day with 1 evaluator; or 1 day with a lead evaluator and an expert may be more effective than 1 day without the expert) (see IAF MD 5:2015 subs 2.2.4).

6.2 Calculation of the determination time

6.2.1 Factors in the calculation

The following two (possibly mutually dependent) factors are crucial in calculating the determination time:

1) Number of employees involved in the data processing operation or operations. This factor is significant because, among other things, competence, awareness of policies and instructions, and correct execution of organisational processes need to be verified. In addition, the number of employees is an indicator of the volume of data processing.
2) Number of cloud users who use the cloud service. If the cloud service is used by a large number of users, not only is there more application and usage data that requires special protection (see Section VII of the AUDITOR Criteria Catalogue), but the number of data subjects also tends to increase. In addition, the number of legally binding agreements to be reviewed and the scope of precautions to safeguard the rights of data subjects also increase.

Additional aspects, including those specific to the cloud service, should also be considered when calculating the determination time. These include, but are not limited to:

(1) the complexity of the cloud provider and the data processing operations;
(2) the requested protection category and restorability class;
(3) the number of sites, their geographical location and multiple site considerations;
(4) the technological and organisational context, including
  (a) the TOM of the cloud provider within the meaning of Art. 28 of the GDPR;
  (b) the technology and IT landscape in use, including relevant IT systems;
  (c) the organisational processes for carrying out the data processing operations;
  (d) the outsourced development work;
(5) cloud supply chain nesting, outsourced operations and interfaces with subcontracted processors;
(6) specific data protection risks of the data processing operations.

6.2.2 Example of a determination time chart

The determination time chart below provides a guide to an average number of determination days. The chart provides a framework for determination planning by establishing a starting point based on the total number of personnel and number of cloud users for all protection categories. This determination time chart must consider factors that require adjustment or limitation of the determination time (see 6.2.3 and 6.2.4 below). The determination time chart also allocates the determination days according to protection categories, based on the assumption of a 10% increase for protection category 2 and a 20% increase for protection category 3 compared to the determination days for protection category 1, rounded up to the next higher day.

The certification body takes account of both factors (number of employees and number of cloud customers), provided that that information is available, and selects the higher number of determination days specified for the two factors. For example, during determination planning, it is determined that 14 employees work at the cloud provider and 10 cloud customers use the service. For protection category 2, this results in an average of 7 determination days, as the number of employees in this case gives the higher number of determination days.

Number of employees	Number of cloud customers	Time required per protection category (SK) in determination days		
		SK 1	SK 2	SK 3
1~10	1~10	5	6	6
11~15	11~25	6	7	8
16~25	26~50	7	8	9
26~45	51~100	8,5	10	11
46~65	101~150	10	11	12
66~85	151~250	11	13	14
86~125	251~500	12	14	15
126~175	501~1000	13	15	16
176~275	1.001~1.750	14	16	17
276~425	1.751~3.000	15	17	18
426~625	3.001~5.000	16.5	19	20
626~875	5.001~10.000	17.5	20	21
876~1.175	10.000~17.500	18.5	21	23
1.176~1.550	17.501~25.000	20	22	24
> 1.550	> 25.000	Follows the progression above	Follows the progression above	Follows the progression above

6.2.3 Factors requiring adjustment of the determination time

The determination time chart must not be used in isolation. The certification body must consider other factors which, on the one hand, require additional determination time or, on the other hand, lead to a reduction in the determination time.

Factors that extend the determination time include the following:

- Determination covering recoverability class 2: usually requires an additional time of 0.25 determination days.
- Determination covering recoverability class 3: usually requires an additional time of 0.5 determination days.

- Determination covering multiple sites (e.g. multiple data centres or outsourced development teams; see § 5.2.6).
- Processing operations covering highly complex procedures or a relatively large number of unique activities.
- Personnel speaking more than one language (requiring one or more interpreters or preventing individual evaluators from working independently) or documents submitted in more than one language.
- Outsourcing of a large number of functions or processes or use of a large number of subcontracted processors.
- Complaints from the past, surveillance results or previous experience with the data processing operation indicating a need for more determination time.

Examples of factors that allow for a shorter determination time include:

- Low data protection risks of data processing (e.g. due to pseudonymisation and anonymisation procedures) or activities of low complexity.
- A high percentage of people working under the control of the cloud provider and performing the same tasks.
- Prior knowledge and a high level of preparedness of the cloud provider (e.g. if the cloud provider has already been certified by the same certification body according to another standard).
- Recognition of existing certificates (see § 5.1.7), so that only a sample determination of a large number of criteria is necessary.
- A large number of criteria not being applicable to the certification object (see § 5.1.5).
- A very small site in relation to the number of employees (e.g., only one office complex).
- A high degree of automation.

Factors that increase the determination time can be offset by factors that reduce the time. The decimal number obtained in the result of the calculation should be rounded up or down to the nearest half day (e.g., 5.3 determination days become 5.5 determination days; 5.2 determination days become 5 determination days; see IAF MD5:2015 subs. 2.2.3).

6.1.3 Limiting variations in the determination time

In order to ensure that the determination is carried out effectively and to guarantee reliable and comparable results, the determination time indicated in the determination schedule may not be reduced by more than 30%.

In all cases where adjustments are made to the time allowed for the determination, sufficient evidence (including justification for deviations) and records must be kept justifying the change. The certification body is required to ensure that any changes to the determination time do not compromise the effectiveness of the certification.

The certification body reports annually to the scheme owner on the determination times calculated and invoiced for certification (see § 4.4.4). On request by the scheme owner, the certification body is required to provide justification for this.

7 References

Decision No 768/2008/EC	Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products and repealing Council Decision 93/465/EEC (Text with EEA relevance); http://data.europa.eu/eli/dec/2008/768(1)/oj
DAkkS 71 SD 0 001	General rules for accreditation of conformity assessment bodies. Revision: 1.3 | 29 August 2012
DAkkS 71 SD 0 013	Specifications for the application of DIN EN ISO/IEC 17065 in accreditation of bodies that accredit products, processes and certify services. Revision: 1.1 | 04 December 2014
DAkkS 71 SD 0 016	Regulation for determining accreditation eligibility of new private conformity assessment schemes according to point 4.6.3 EN ISO/IEC 17011. Revision: 1.3 | 27.11.2018
DSK	Requirements for accreditation according to Art. 43(3) GDPR in conjunction with DIN EN ISO/IEC 17065. Version 1.4 (08.10.2020).
DSK ADZ	Requirements for certification programs under data protection law. Data protection test criteria, test systems and test methods for the adaptation and application of the technical standard DIN EN ISO/IEC 17067 (programme type 6). Version 1.8 (16.04.2021)
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 at 04.06.2019
IAF MD 2:2017	IAF mandatory document for the transfer of accredited certification of management systems. Issue 2.
IAF MD 4:2018	IAF mandatory document for the use of information and communication technology (ICT) for auditing/assessment purposes Issue 2. as of 2018.
IAF MD 5:2015	Determination of audit time of quality, environmental and occupational health & safety management systems. Issue 4, Version 2.
IAF MD 1:2018	IAF mandatory document for audit and certification of a management system operated by a multi-site organisation. Issue 2.
IAF/ILAC A5:11/2013	IAF/ILAC Multi-lateral mutual recognition arrangements (Arrangements): Application of ISO/IEC 17011:2004. 2013 revision.
ISO/IEC 15408:2009	Information technology -- Security techniques -- Evaluation criteria for IT security. Status 2009
ISO/IEC 17000:2004	Conformity assessment - Vocabulary and general principles. Status 2004.
ISO/IEC 17020:2012	Conformity assessment - Requirements for the operation of various types of bodies performing inspection. Status 2012
ISO/IEC 17021-1:2015	Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements. Status 2015
ISO/IEC 17024:2012	Conformity assessment - General requirements for bodies operating certification of persons. Status 2012
ISO/IEC 17025:2017	General requirements for the competence of testing and calibration laboratories. Status 2017
ISO/IEC 17030:2009	Conformity assessment - General requirements for third-party marks of conformity. Status 2009
ISO/IEC 17040:2005	Conformity assessment - General requirements for peer assessment of conformity assessment bodies and accreditation bodies. Status 2005
ISO/IEC 17065:2012	Conformity assessment - Requirements for bodies certifying products, processes and services. Status 2012
ISO/IEC 17067:2013	Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes. Status 2013
ISO/IEC 18045:2008-018	Information technology — Security techniques — Methodology for IT security evaluation. Status 2008
ISO 19011:2018	Guidelines for auditing management systems. Status 2018

Lins et al. (2016)	Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic Certification of Cloud Services: Trust, but Verify! IEEE Security and Privacy, 14(2), 67-71. https://doi.org/10.1109/MSP.2016.26
Lins et al. (2019)	Lins, S., Schneider, S., Szefer, J., Ibraheem, S., & Sunyaev, A. (2019). Designing Monitoring Systems for Continuous Certification of Cloud Services: Deriving Meta-requirements and Design Guidelines. Communications of the Association for Information Systems, 44. https://doi.org/10.17705/1CAIS.04425
Information sheet on accreditation procedures in data protection	Information sheet on accreditation procedures in data protection. Status 13.03.2020. https://www.dakks.de/content/merkblatt-zu-akkreditierungsverfahren-im-datenschutz
NIST (2011)	Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing. https://csrc.nist.gov/publications/detail/sp/800-145/final