European Cloud Service
Data Protection Certification

AUDITOR-Konformitätsbewertungs-Programm

- Fassung 0.99 -

Stand 15.01.2020

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Kriterienkatalog (https://doi.org/10.5445/IR/1000105506)
- Ermittlungsmethoden
- Modularitätskonzept
- Schutzklassenkonzept
- DIN SPEC 27557

Online verfügbar: www.auditor-cert.de

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Energie gefördert wird (FKZ 01MT17003A).

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Autoren

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

[a] Forschungsgruppe Critical Information Infrastructures am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

[b] Projektgruppe verfassungsverträglichen Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
DAkkS	Deutsche Akkreditierungsstelle GmbH
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
DSK	Datenschutzkonferenz
i.S.d.	Im Sinne des
IaaS	Infrastucture as a Service
Lit.	Litera
Nr.	Nummer
PaaS	Platform as a Service
s.	siehe
SaaS	Software as a Service
TCDP	Trusted Cloud Datenschutz-Profil
TOM	technische und organisatorische Maßnahmen

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen im AUDITOR-Konformitätsbewertungsprogramm sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z.B. ist bei der Bezeichnung *Evaluator* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

1 Einleitung

1.1 Funktion und Ziele des AUDITOR-Konformitätsbewertungsprogramm

Die AUDITOR-Zertifizierung liefert einen Nachweis über die Konformität von Datenverarbeitungsvorgängen von Cloud-Anbietern mit den Anforderungen der EU-Datenschutzgrundverordnung (DSGVO). Gemäß Art. 43 Abs. 1 Satz 1 DSGVO können Zertifizierungsstellen neben Datenschutz-Aufsichtsbehörden Zertifizierungen erteilen. Eine Zertifizierungsstelle darf ihre Tätigkeit jedoch nur aufnehmen, wenn sie durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) in Zusammenarbeit mit der zuständigen Datenschutz-Aufsichtsbehörde akkreditiert wurde. Voraussetzung der Akkreditierung ist die Einhaltung der Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der Datenschutzkonferenz (DSK) zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065.

Maßgeblich für die Akkreditierung ist ein Konformitätsbewertungsprogramm, das für jedes Zertifizierungsverfahren erstellt werden muss. Das Konformitätsbewertungsprogramm beschreibt die spezifischen Anforderungen, Regeln sowie Prüfverfahren, die zur Konformitätsbewertung von Datenverarbeitungsvorgängen verwendet werden müssen, um die mit der Zertifizierung verbundene Aussage, auf wissenschaftlich rückführbare und systematische Weise treffen zu können (s. DAkkS 71 SD 0 016). Das vorliegende *‚AUDITOR-Konformitätsbewertungsprogramm‘* beschreibt daher die von der Zertifizierungsstelle zu erfüllenden Grundsätze und umfasst im Wesentlichen Anforderungen an die Zertifizierungsstelle und den Zertifizierungsprozess. Das AUDITOR-Konformitätsbewertungsprogramm wird zukünftig durch das Kompetenznetzwerk Trusted Cloud e.V. als Programmeigner verwaltet und weiterentwickelt. Es wird interessierten Zertifizierungsstellen zu nicht-diskriminierenden Bedingungen zur Verfügung gestellt, um eine breite Anwendung des Zertifizierungsverfahrens sicherzustellen.

1.2 Fortentwicklung vom TCDP gemäß der Datenschutz-Grundverordnung

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte Trusted Cloud Datenschutz-Profil (TCDP) untersucht. Da bei der Entwicklung der Zertifizierungskriterien nach TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke – z. B. Cloud Computing Compliance Controls Catalogue (C5) – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, muss mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25.5.2018 das TCDP-Kriterienwerk an die neuen Regelungen angepasst werden. Dies geschieht mit dem *‚AUDITOR-Kriterienkatalog‘*, welcher alle relevanten Vorschriften für die Datenschutz-Zertifizierung von Cloud-Diensten in der Datenschutz-Grundverordnung fokussiert und diese zu prüffähigen Kriterien konkretisiert.

Im Rahmen des Pilotprojekts wurde auch eine Verfahrensordnung für Zertifizierungen nach dem TCDP erstellt. Eine Akkreditierung dieser Verfahrensordnung wurde jedoch nicht vorgenommen. Diese Verfahrensordnung wurde bei der Entwicklung des AUDITOR-Konformitätsbewertungsprogramms berücksichtigt. Eine Anpassung der TCDP-Verfahrensordnung ist in Hinblick auf die Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065 erforderlich und wird durch das AUDITOR-Konformitätsbewertungsprogramm adressiert.

1.3 Aufbau und Inhalte des Konformitätsbewertungsprogramms

Das AUDITOR-Konformitätsbewertungsprogramm gliedert sich in vier wesentliche Kapitel. In Kapitel 2 werden der Zweck des Konformitätsbewertungsprogramms festgelegt sowie zentrale Begriffe definiert. Kapitel 3 regelt die Grundsätze zur Durchführung von Zertifizierungstätigkeiten, um unter anderem Vertrauen in die Tätigkeiten und Ergebnisse zu schaffen. Kapitel 4 legt Anforderungen an die Zertifizierungsstelle fest, darunter bspw. Anforderungen an Struktur und Ressourcen der Zertifizierungsstelle. Kapitel 5 beschreibt Anforderungen an den Zertifizierungsprozess, aufgegliedert in die Prozessphasen Auswahl, Ermittlung, Bewertung, Entscheidung, Bestätigung und Überwachung.

Bei der Spezifikation eines Konformitätsbewertungsprogramms ist die Festlegung der Prüfung der einzelnen Kriterien wesentlich, um sicherzustellen, dass verschiedene Prüfer zum gleichen Ergebnis der Konformitätsbewertung kommen. Aus diesem Grund wird pro Kriterium im Begleitdokument *‚AUDITOR-Ermittlungsmethoden‘* angegeben, wie das jeweilige Kriterium zu prüfen ist.

2 Grundlagen

2.1 Das AUDITOR-Konformitätsbewertungsprogramm

§ 2.1.1 Bezeichnung des Konformitätsbewertungsprogramms

(1) Die vorläufige Bezeichnung dieses Programms lautet: AUDITOR-Konformitätsbewertungsprogramm.

(2) Der Name der Zertifizierung wird zurzeit abgestimmt. Es wird ein Markenschutz auf europäischer Ebene angestrebt. Der Programmeigner informiert die DAkkS über die finale Festlegung des Namens.

§ 2.1.2 Zweck des Konformitätsbewertungsprogramms

(1) Ziel der AUDITOR-Zertifizierung ist es Vertrauen in die Datenverarbeitung von Cloud-Diensten bei der Verarbeitung von personenbezogenen Daten zu schaffen.

(2) Die AUDITOR-Zertifizierung liefert einen Nachweis über die Konformität von Datenverarbeitungsvorgängen von Cloud-Anbietern mit den Anforderungen der Datenschutz-Grundverordnung.

(3) Dieses Konformitätsbewertungsprogramm legt Anforderungen an die Zertifizierungsstelle und die Durchführung des Zertifizierungsprozesses fest, deren Einhaltung sicherstellen soll, dass das AUDITOR-Zertifizierungsverfahren durch die Zertifizierungsstellen kompetent, konsequent und unparteiisch betrieben wird.

(4) Durch dieses Konformitätsbewertungsprogramm soll zudem sichergestellt sein, dass die Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065 eingehalten werden.

§ 2.1.3 Konformitätsbewertungsart

(1) Dieses Konformitätsbewertungsprogramm unterfällt der Konformitätsbewertungsart „Zertifizierung“ im Sinne der ISO/IEC 17065:2012.

(2) Dieses Programm fällt im Sinne der ISO/IEC 17067:2013 Tz. 5.3.8 unter den Programmtyp 6.

§ 2.1.4 Programmeigner

(1) Der Programmeigner ist eine Person oder Organisation, die für die Entwicklung und Aufrechterhaltung dieses Konformitätsbewertungsprogramms verantwortlich ist (s. ISO/IEC 17065:2012 Tz. 3.11). Der Programmeigner vereinbart und überwacht durch eine rechtlich bindende Vereinbarung mit akkreditierten Zertifizierungsstellen, die Einhaltung der Zertifizierungsanforderungen zur Vergabe von Konformitätszeichen (s. DAkkS 71 SD 0 016).

(2) Der Programmeigner dieses Konformitätsbewertungsprogram ist das Kompetenznetzwerk Trusted Cloud e.V. Beim Kompetenznetzwerk Trusted Cloud e.V. ist ein Beirat zur Durchführung, der Leitung und Lenkung dieses Programms eingerichtet (s. ISO/IEC 17067:2013 Tz. 6.3.5). Der Beirat stellt das Beschlussorgan über

   (a) Änderungen/Ergänzungen des AUDITOR-Kriterienkatalogs,
   (b) Änderungen des AUDITOR-Konformitätsbewertungsprogramms,
   (c) Fragen der Internationalisierung und Standardisierung, und
   (d) bei Kooperationen dar,

   und nimmt eine beratende Funktion bei allen Fragen der Marktansprache und Lizensierung der Zertifizierung ein. *Die Zusammensetzung des Beirats befindet sich zurzeit in Abstimmung.*

(3) Der Programmeigner übernimmt die volle Verantwortung für die Ziele, den Inhalt und die Vollständigkeit dieses Programms (s. ISO/IEC 17067:2013 Tz. 6.3.4).

(4) Der Programmeigner pflegt dieses Programm und gibt bei Bedarf Anleitung für Zertifizierungsstellen (s. ISO/IEC 17067:2013 Tz. 6.3.5). Dazu werden folgende Aktivitäten ausgeführt:

   (a) Durchführung von Änderungen an den festgelegten Zertifizierungskriterien (s. ISO/IEC 17067:2013 Tz. 6.6.2);
   (b) Leitung der Standardisierungsaktivitäten der Zertifizierungskriterien (bspw. Überführung in DIN-, EU- oder ISO-Norm).;
   (c) Durchführung von Änderungen an diesem Konformitätsbewertungsprogramm;
   (d) Beobachtung von

(i) Änderungen der rechtlichen Rahmenbedingungen, die sich durch Gesetzesnovellierungen, den Erlass delegierter Rechtsakte der Europäischen Kommission, Entscheidungen des Europäischen Datenschutzausschusses und Gerichtsentscheidungen ergeben;
(ii) Fortentwicklungen des Stands der Technik;
(iii) Änderungen von Anforderungen der Datenschutz-Aufsichtsbehörde und des Datenschutzausschusses an Kriterienkatalogen und Zertifizierungsverfahren;
(iv) Rechtsakten und anderen Vorgaben von dem Datenschutzausschuss oder Datenschutz-Aufsichtsbehörden.

(e) Informieren der akkreditierten Zertifizierungsstellen bei relevanten bzw. wesentlichen Änderungen;
(f) Koordination von Kooperationen mit Interessengruppen zur Pflege und Weiterentwicklung des Programms und der Zertifizierungskriterien;
(g) Durchführung und Koordination von Tätigkeiten zur Internationalisierung der Zertifizierung, bspw. Einreichung als Europäischen Datenschutzsiegel beim EU-Ausschuss;
(h) Beratende Aktivitäten bei allen Fragen der Marktansprache;
(i) Informationsaustausch und Abstimmung mit der DAkkS, DSK, AK Zertifizierung und nationalen Datenschutz-Aufsichtsbehörden.

(5) Der Programmeigner schätzt die Risiken/Verbindlichkeiten, die aus seinen Tätigkeiten entstehen, ein und handhabt diese entsprechend (s. ISO/IEC 17067:2013 Tz. 6.3.10).
(6) Der Programmeigner stellt sicher, dass Informationen über dieses Programm der Öffentlichkeit zugänglich gemacht werden, um Transparenz, Verständnis und Akzeptanz sicherzustellen (s. ISO/IEC 17067:2013 Tz. 6.4.5). Hierzu werden folgende Maßnahmen durchgeführt:

(a) Veröffentlichung der Zertifizierungskriterien im AUDITOR-Kriterienkatalog mit freiem Zugang für alle Interessengruppen auf dem Internetportal der Zertifizierung;
(b) Veröffentlichung dieses Programms mit Zugang für Cloud-Anbieter, Datenschutz-Aufsichtsbehörde, Zertifizierungsstellen und bei Bedarf für weitere Interessengruppen durch elektronische Übermittlung des Programms.

§ 2.1.5 Anwendungsbereich

(1) Dieses Konformitätsbewertungsprogramm enthält Zertifizierungsanforderungen an die Kompetenz, die einheitliche Arbeitsweise und die Unparteilichkeit von Zertifizierungsstellen für die Datenschutzzertifizierung von Datenverarbeitungsvorgängen in Cloud-Diensten gemäß den Anforderungen der Datenschutz-Grundverordnung.
(2) Die Zertifizierung nach AUDITOR steht allen privatwirtschaftlichen Cloud-Anbietern offen, die als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO agieren und die Konformität ihrer Datenverarbeitungsvorgänge mit der Datenschutz-Grundverordnung nachweisen wollen.
(3) Die Zertifizierungskriterien werden in der maßgeblichen Fassung des AUDITOR-Kriterienkatalog festgelegt.
(4) Das Konformitätsbewertungsprogramm wird interessierten Zertifizierungsstellen zu nicht-diskriminierenden Bedingungen zur Verfügung gestellt, um eine Akkreditierung nach diesem Programm zu ermöglichen und eine breite Anwendung des Zertifizierungsverfahrens sicherzustellen.

§ 2.1.6 Änderungen an diesem Konformitätsbewertungsprogramm

(1) Änderungen an diesem Konformitätsbewertungsprogramm werden durch den Programmeigener durchgeführt.
(2) Der Programmeigner verpflichtet sich, zukünftige Änderungen des Programms über geeignete Kommunikationskanäle den akkreditierten Zertifizierungsstellen, nach diesem Programm zertifizierten Cloud-Anbietern, Datenschutz-Aufsichtsbehörde und der DAkkS sowie bei Bedarf weiteren Interessengruppen frühzeitig mittzuteilen. Wurden die Änderungen genehmigt (i.d.R. durch die DAkkS und zuständige Datenschutzaufsichtsbehörde) werden die akkreditierten Zertifizierungsstellen und zertifizierten Cloud-Anbieter ebenfalls zeitnah informiert.

§ 2.1.7 Entwicklungshistorie

(1) Das Konformitätsbewertungsprogramm wurde im Rahmen des Forschungsprojekts AUDITOR durch die Forschungsgruppe Critical Information Infrastructures von Prof. Dr. Ali Sunyaev und den Mitarbeitern Sebastian Lins und Heiner Teigeler an dem Karlsruher Institut für

Technologie und der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) unter der Leitung von Prof. Dr. Alexander Roßnagel und der Mitarbeiterin Dr. Natalie Maier an der Universität Kassel entwickelt.

(2) Weitere Parteien wirkten an der Überarbeitung und Ausgestaltung dieses Programms mit, darunter:

(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) Kompetenznetzwerk Trusted Cloud e.V.;
(g) sowie weitere assoziierte Partner des Projektes.

2.2 Begrifflichkeiten

§ 2.2.1 Zertifizierungsstelle

(1) Die Zertifizierung nach AUDITOR erfolgt durch eine unabhängige und fachlich geeignete Zertifizierungsstelle, welche im Sinne einer Konformitätsbewertungsstelle als dritte Seite auftritt (s. ISO/IEC 17000:2004 Tz. 2.5, DSK Tz. 4.2.1).

(2) Die Zertifizierungsstelle muss eine rechtsfähige Organisation oder ein abgegrenzter Teil einer rechtsfähigen Organisation sein. Gemäß Artikel R 17 Abs. 3 S. 1 des Beschlusses Nr. 768/2008/EG muss es sich bei einer Zertifizierungsstelle um einen unabhängigen Dritten handeln, der mit der Einrichtung, die er bewertet, in keinerlei Verbindung steht (s. DSK Tz. 4.2.1).

(3) Die Zertifizierungsstelle führt ihre Tätigkeit nicht-diskriminierend, vertraulich und unparteilich aus.

(4) Zertifizierungsstellen müssen sich nach der ISO/IEC 17065 i.V.m. den ergänzenden Anforderungen zur Akkreditierung nach Art. 43 Abs. 3 DSGVO und diesem Programm akkreditieren lassen, um damit die Erfüllung der Zertifizierungsanforderungen, insbesondere die Erfüllung der Grundsätze, nachzuweisen.

(5) Die Zertifizierungsstelle steht in einem Vertragsverhältnis mit dem zu zertifizierenden Cloud-Anbieter und ggf. zu ausgegliederten Evaluatoren.

§ 2.2.2 Evaluierung

(1) Evaluierung bezeichnet die Konformitätsbewertungsfunktionen Auswahl und Ermittlung (s. ISO/IEC 17065:2012 Tz. 3.3).

§ 2.2.3 Evaluatoren

(1) Evaluatoren im Sinne dieses Programms sind natürliche Personen, die der Zertifizierungsstelle angehören und die Auswahl- und/oder Ermittlungstätigkeiten nach diesem Programm durchführen.

(2) Eine Zertifizierungsstelle kann zudem eine ausgegliederte, unabhängige und fachlich kompetente Prüfstelle oder (einzelne) externe Evaluatoren zur Durchführung der Auswahl- und/oder Ermittlungstätigkeiten gemäß ISO/IEC 17065:2012 Tz. 6.2.2 benennen (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Mittarbeiter dieser Prüfstellen und externe Evaluatoren werden entsprechend als ausgegliederte Evaluatoren bezeichnet. Sie führen ihre Tätigkeit nichtdiskriminierend, vertraulich und unparteilich aus.

(3) Prüfstellen und ausgegliederte Evaluatoren haben ein Vertragsverhältnis mit der Zertifizierungsstelle. Ein Vertragsverhältnis darf nicht mit einem zu zertifizierenden Cloud-Anbieter bestehen (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

§ 2.2.4 Entscheider

(1) Entscheider im Sinne dieses Programms sind natürliche Personen, die der Zertifizierungsstelle angehören und die die Bewertung und/oder die Entscheidung über die Zertifizierung und/oder anschließend die Genehmigung der Zertifizierung durchführen.

§ 2.2.5 Akkreditierungsstelle

(1) Eine Akkreditierungsstelle ist eine befugte Stelle, die Akkreditierungen durchführt (s. ISO/IEC 17000:2004 Tz. 2.6).

(2) Eine Akkreditierung ist eine Bestätigung durch eine dritte Seite, die formal darlegt, dass eine Konformitätsbewertungsstelle (hier Zertifizierungsstelle) die Kompetenz besitzt, bestimmte

Konformitätsbewertungsaufgaben (hier Zertifizierung) durchzuführen (s. ISO/IEC 17000:2004 Tz. 5.6).

(3) In Deutschland ist die DAkkS alleinig zuständig für die Durchführung von Akkreditierungen.

§ 2.2.6 Gegenstand der Bewertung/Zertifizierungsgegenstand

(1) Gegenstand der Bewertung (i.S.d. Tz. A.2.2 ISO/IEC 17000:2004, Anhang A) sind Datenverarbeitungsvorgänge mit personenbezogenen Daten i.S.d. Art. 4 Nr. 1 DSGVO, die in Cloud-Diensten oder mit Hilfe von (auch mehreren) Cloud-Diensten erbracht werden.

(2) Das Begleitdokument *„AUDITOR-Zertifizierungsgegenstand“* zu diesem Programm enthält eine detaillierte Herleitung und Beschreibung des Zertifizierungsgegenstandes. Zertifizierungsstellen und (ausgegliederte) Evaluatoren müssen sich mit diesem Begleitdokument vertraut machen.

§ 2.2.7 Cloud-Dienste

(1) Cloud-Dienste im Sinne dieses Konformitätsbewertungsprogramms sind Cloud-Dienste gemäß der Definition des National Institute of Standards and Technology (NIST).

(2) Cloud-Dienste ermöglichen einen flexiblen und bedarfsorientierten Zugriff auf einen gemeinsam genutzten Pool von konfigurierbaren IT-Ressourcen, die jederzeit und überall über das Internet oder ein Netzwerk abgerufen werden können.

(3) Die für Cloud-Dienste kennzeichnenden Charakteristiken sind der bedarfsgerechte Zugriff, eine Netzwerkanbindung, die Möglichkeit zur Ressourcenbündelung, eine hohe Skalierbarkeit und eine verbrauchsabhängige Bezahlung:

   (a) Bedarfsgerechter Zugriff: Der bedarfsgerechte Zugriff ermöglicht es Cloud-Nutzern selbstständig und nahezu unmittelbar Leistungsparameter der in Anspruch genommenen Cloud-Dienste anzupassen. Dies kann insbesondere automatisch und ohne menschliche Interaktion mit den jeweiligen Cloud-Anbietern durchgeführt werden.
   (b) Netzwerkanbindung: Cloud-Dienste werden über ein Breitbandnetzwerk bereitgestellt, in der Regel über das Internet.
   (c) Skalierbarkeit: Bereitgestellte Ressourcen können flexibel und schnell, in einigen Fällen vollautomatisch, erhöht oder freigegeben werden, um so die Ressourcen auf den aktuellen Bedarf abzustimmen.
   (d) Verbrauchsabhängige Bezahlung: Um Cloud-Dienste messbar und transparent zu gestalten, kontrollieren und optimieren Cloud-Dienste den Ressourcenverbrauch anhand von service-abhängigen Kennzahlen, bspw. dem Speicherplatz, der Rechenleistung oder der Bandbreite. Dadurch kann eine bedarfsgerechte Abrechnung angeboten und durchgeführt werden. Zudem wird die Ressourcennutzung überwacht, kontrolliert, protokolliert und kommuniziert, sodass sowohl für die Cloud-Nutzer als auch für den Cloud-Anbieter, Transparenz über die Nutzung geschaffen wird.

(4) Im Rahmen dieses Konformitätsbewertungsprogramms wird zwischen den drei grundlegenden Dienstmodellen Software as a Service (SaaS), Platform as a Service (PaaS) sowie Infrastructure as a Service (IaaS) unterschieden. Darüber hinaus finden sich in der Praxis und Literatur eine Vielzahl von weiteren Dienstmodellen, bspw. Database as a Service oder Security as a Service. Allerdings lassen sich diese spezifischen Dienstmodelle im Allgemeinen den grundlegenden Modellen Infrastructure, PaaS und SaaS zuordnen.

   (a) SaaS. Der Cloud-Nutzer kann mittels verschiedener Geräte entweder über ein Thin-Client-Interface, bspw. einen Web-Browser, oder über ein entsprechendes Anwendungsinterface auf angebotene Softwareanwendungen zugreifen.
   (b) PaaS. Der Cloud-Nutzer kann selbstentwickelte oder erworbene Anwendungen auf der Cloud-Infrastruktur des Cloud-Anbieters installieren und betreiben. Hierzu werden Betriebssysteme, Datenbanken, Programmierumgebungen, Programmbibliotheken oder weitere vom Cloud-Anbieter unterstützte Dienste und Werkzeuge genutzt.
   (c) IaaS. Der Cloud-Nutzer erhält Zugang zu Hardwareressourcen des Cloud-Anbieters, darunter fallen bspw. Rechenleistung, Speicherkapazitäten oder Netzwerke. Diese kann er zur Installation und zum Betrieb beliebiger Software verwenden, bspw. Betriebssysteme oder Anwendungen.

(5) Cloud-Dienste können ferner Bestandteil von anderen Cloud-Diensten sein, sodass in der Praxis vermehrt verschachtelte Wertschöpfungsketten oder -netzwerke von Cloud-Diensten

auftreten. Die Verantwortlichkeiten des Cloud-Dienstes und die Abhängigkeiten und Schnittstellen zu anderen Cloud-Diensten sind im Rahmen der Zertifizierung daher klar zu benennen und abzugrenzen.

(6) Cloud-Dienste sind Dienstleistungen im Sinne der ISO/IEC 17065:2012.

(7) Das Begleitdokument *„AUDITOR-Zertifizierungsgegenstand*" zu diesem Programm enthält eine detaillierte Beschreibung von Cloud-Diensten in Bezug auf den Zertifizierungsgegenstand.

§ 2.2.8 Datenverarbeitungsvorgänge in Cloud-Diensten

(1) Eine Datenverarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

(2) Ein Datenverarbeitungsvorgang kann sowohl technische und automatisierte als auch nichttechnische und somit auch organisatorische (bspw. manuelle oder personelle) Vorgangsschritte enthalten, worunter auch Datenschutzkonzepte und -managementsysteme fallen können.

(3) Der gesamte Verarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

(4) Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können.

(5) Die Eignung eines Datenverarbeitungsvorgangs für die AUDITOR-Zertifizierung wird im Rahmen der Auswahltätigkeiten überprüft (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

(6) Das Begleitdokument *„AUDITOR-Zertifizierungsgegenstand"* zu diesem Programm enthält eine detaillierte Beschreibung von Datenverarbeitungsvorgängen in Cloud-Diensten in Bezug auf den Zertifizierungsgegenstand.

§ 2.2.9 Cloud-Anbieter

(1) Cloud-Anbieter sind Rechtsträger, die Cloud-Dienste betreiben.

(2) Cloud-Anbieter stellen die Kunden der Zertifizierungsstelle dar.

(3) Cloud-Anbieter sind gegenüber einer Zertifizierungsstelle verantwortlich dafür, sicherzustellen, dass die Zertifizierungskriterien erfüllt sind (s. ISO/IEC 17065:2012 Tz. 3.1).

§ 2.2.10 Subauftragsverarbeiter

(1) Ein Cloud-Anbieter kann im Rahmen seiner Datenverarbeitungsvorgänge weitere Subauftragsverarbeiter einbeziehen, die externe Ressourcen und Dienstleistungen für die Durchführung der Datenverarbeitungsvorgänge bereitstellen.

(2) Subauftragsverarbeiter sind Rechtsträger, die Produkte oder Dienstleistungen betreiben, welche relevant für die zu zertifizierenden Datenverarbeitungsvorgänge sind.

(3) Ein Subauftragsverarbeiter ist unabhängig von dem Cloud-Anbieter.

(4) Setzen die zu zertifizierenden Verarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Cloud-Anbieter sonstige Subauftragsverarbeiter ein, so kann sich die Zertifizierung nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Cloud-Anbieters stehen. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass auch diese fremden von ihm genutzten Plattformen, Infrastrukturen und Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Dienstes einsetzen.

§ 2.2.11 Cloud-Nutzer

(1) Cloud-Nutzer im Sinne dieses Programms ist jede natürliche und juristische Person, die als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO Verarbeitungen personenbezogener Daten

durchführt und allein oder gemeinsam mit anderen über Zwecke und Mittel dieser Verarbeitungen entscheidet und sich entschließt, diese Verarbeitungen an einen Cloud-Anbieter auszulagern.

(2) Cloud-Nutzer stellen somit die Kunden des Cloud-Anbieters dar.

§ 2.2.12 Datenschutz-Aufsichtsbehörde

(1) Eine Datenschutz-Aufsichtsbehörde ist eine von einem Mitgliedstaat gemäß Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle (s. Art. 4 Abs. 21 DSGVO).

(2) Als zuständige Datenschutz-Aufsichtsbehörde wird eine Datenschutz-Aufsichtsbehörde bezeichnet, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

(a) der Cloud-Nutzer als Verantwortlicher oder der Cloud-Anbieter als Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Datenschutz-Aufsichtsbehörde niedergelassen ist,

(b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Datenschutz-Aufsichtsbehörde hat oder haben kann oder,

(c) eine Beschwerde bei dieser Datenschutz-Aufsichtsbehörde eingereicht wurde (s. Art. 4 Abs. 22 DSGVO).

(3) Die DAkkS akkreditiert als Akkreditierungsstelle die Zertifizierungsstellen gemeinsam mit der zuständigen Datenschutzaufsichtsbehörde. Die zuständige Datenschutzaufsichtsbehörde erteilt der Zertifizierungsstelle in einem eigenständigen Verfahren auf Grundlage dieser gemeinsamen Akkreditierung die Befugnis als solche tätig werden zu dürfen (s. DSK ‚Vorwort').

§ 2.2.13 Europäischer Datenschutzausschuss

(1) Der Europäische Datenschutzausschuss wurde als Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit eingerichtet und besteht aus dem Leiter einer Datenschutz-Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern (s. Art. 68 Abs. 1 und 3 DSGVO).

(2) Der Europäische Datenschutzausschuss kann die Zertifizierungskriterien genehmigen, sodass dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führt.

§ 2.2.14 Zertifizierungskriterien

(1) Zertifizierungskriterien sind die im AUDITOR-Kriterienkatalog festgelegten normativen Anforderungen, die durch den Cloud-Anbieter als Bedingung zur Feststellung oder Aufrechterhaltung der Zertifizierung erfüllt sein müssen.

(2) Die genehmigten Kriterien werden im Sinne des Art. 42 Abs. 5 DSGVO unter Angabe des jeweiligen Verwendungszeitraums durch den Programmeigner in einer elektronischen Form veröffentlicht (s. DSK Tz. 4.6, EDPB Annex 1 Tz. 4.6).

§ 2.2.15 Zertifizierungsanforderungen

(1) Anforderungen an die Zertifizierungsstelle und das Zertifizierungsverfahren, welche durch dieses Konformitätsbewertungsprogramm vorgegeben sind.

§ 2.2.16 Schutzklassen

(1) Der AUDITOR-Kriterienkatalog nimmt bei einigen Kriterien eine Unterscheidung nach Schutzklassen vor und legt für diese unterschiedliche Zertifizierungskriterien fest, die erfüllt werden müssen. Schutzklassen stellen bei der AUDITOR-Zertifizierung ein wichtiges Instrument dar, da mit ihnen der individuelle Schutzbedarf von Datenverarbeitungsvorgängen und dessen Erfüllung durch zertifizierte Cloud-Dienste ausgedrückt werden kann.

(2) Bei der Beantragung einer Zertifizierung gibt ein Cloud-Anbieter die für seinen Cloud-Dienst entsprechende Schutzklasse an.

(3) Die Zertifizierungsstelle erstellt auf der Grundlage der Evaluierung eine Bewertung der Erfüllung der Zertifizierungskriterien des AUDITOR-Kriterienkatalogs durch die Datenverarbeitungsvorgänge in Bezug auf eine bestimmte Schutzklasse. Die Zertifizierungsstelle beurteilt jedoch nicht die Wahl der Schutzklasse. Die Schutzklasse wird allein durch den Cloud-Anbieter festgelegt und beantragt und die Zertifizierungsstelle passt entsprechend den Prüfumfang an.

(4) Das Begleitdokument *‚AUDITOR-Schutzklassenkonzept‘* zu diesem Programm enthält eine detaillierte Beschreibung zu den Grundlagen und Ausgestaltungen der Schutzklassen. Zertifizierungsstellen und (ausgegliederte) Evaluatoren müssen sich mit diesem Begleitdokument vertraut machen.

§ 2.2.17 Konformitätszeichen

(1) Geschütztes Zeichen, das von einer Zertifizierungsstelle ausgestellt wird und deutlich macht, dass ein Zertifizierungsgegenstand mit festgelegten Zertifizierungskriterien übereinstimmt (s. ISO/IEC 17030:2009 Tz. 3.1).

(2) Als AUDITOR-Konformitätszeichen werden ein Zertifikat und ein graphisches Gütesiegel vergeben (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**).

§ 2.2.18 Interessierte Parteien

(1) Interessierte Parteien stellen Unternehmen, Privatpersonen, Behörden etc. dar, welche Interesse an der Mitgestaltung oder Mitwirkung der Zertifizierung haben und/oder die Zertifizierung samt ihrer Konformitätszeichen im Markt wahrnehmen.

(2) Interessierte Parteien können insbesondere sein:

(a) Cloud-Nutzer;
(b) Kunden von Cloud-Nutzern;
(c) Datenschutz-Aufsichtsbehörde;
(d) Teilnehmer im Cloud-Markt;
(e) Weitere Zertifizierungsstellen.

3 Grundsätze

Die Zertifizierungsstelle verpflichtet sich die Grundsätze zur Durchführung von Zertifizierungstätigkeiten einzuhalten, um das Vertrauen des Marktes in das AUDITOR-Zertifizierungsverfahren und die erteilten Konformitätszeichen sicherzustellen.

§ 3.1.1 Vermittlung von Vertrauen

(1) Übergeordnetes Ziel der Zertifizierung ist es, allen Beteiligten das Vertrauen zu vermitteln (s. ISO/IEC 17065:2012 Tz. A.1.1), dass Datenverarbeitungsvorgänge in Cloud-Diensten festgelegte Zertifizierungskriterien erfüllen. Der Wert der Zertifizierung ist der Grad an öffentlichem Vertrauen, der durch einen unparteiischen und kompetenten Nachweis einer dritten Stelle vermittelt wird.

(2) Die Zertifizierung soll es Cloud-Anbietern ermöglichen, gegenüber dem Markt nachzuweisen, dass ihren Datenverarbeitungsvorgängen die Erfüllung festgelegter Zertifizierungskriterien durch eine unparteiische dritte Stelle bestätigt wurde (s. ISO/IEC 17067:2013 Tz. 4.2.1).

§ 3.1.2 Unparteilichkeit

(1) Um Vertrauen in ihre Tätigkeiten und Ergebnisse zu schaffen, ist es für die Zertifizierungsstellen und ihr Personal erforderlich, unparteiisch zu sein und als unparteiisch empfunden zu werden (s. ISO/IEC 17065:2012 Tz. A.2.1).

(2) Unparteilichkeit beschreibt das Vorhandensein von Unabhängigkeit und Objektivität (s. ISO/IEC 17025:2017 Tz. 3.1, DSK Tz. 4.2). Unabhängigkeit bedeutet, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann und deren finanzielle Stabilität sichergestellt ist (s. DSK ‚Kapitel 5'). Objektivität bedeutet, dass Interessenkonflikte nicht existieren oder beigelegt wurden, um nachfolgende Zertifizierungstätigkeiten nicht nachteilig zu beeinflussen.

(3) Die Zertifizierungsstelle muss für die Unparteilichkeit ihrer Zertifizierungstätigkeiten verantwortlich sein. Sie darf keinen kommerziellen, finanziellen oder sonstigen Druck zulassen, der die Unparteilichkeit gefährdet.

(4) Die Zertifizierungsstelle ist dafür verantwortlich sicherzustellen, dass auch ausgegliederte Evaluatoren ihre Tätigkeiten unparteiisch durchführen und die Anforderungen zur Unparteilichkeit erfüllen und fortlaufend einhalten. Insbesondere liegt im Regelfall eine unzulässige Gefährdung der Unparteilichkeit vor, wenn Vertragsbeziehungen zwischen zu zertifizierenden Cloud-Anbietern und ausgegliederten Evaluatoren über die Durchführung von Evaluierungstätigkeiten vorliegen.

(5) Risiken für die Unparteilichkeit können Befangenheit miteinschließen, die entstehen kann durch (s. ISO/IEC 17065:2012 Tz. A.2.2):

   (a) Eigennutz (z. B. übermäßige Abhängigkeit von einem Dienstleistungsvertrag oder von den Gebühren oder Angst vor dem Verlust des Cloud-Anbieters oder davor, arbeitslos zu werden, in einem Ausmaß, das die Unparteilichkeit bei der Durchführung der Zertifizierungstätigkeiten nachteilig beeinflusst);
   (b) Selbstbewertung (z. B. Durchführen von Zertifizierungstätigkeiten, bei denen die Zertifizierungsstelle die Ergebnisse anderer Dienstleistungen, die sie bereits erbracht hat, wie z. B. Beratungsdienstleistungen, evaluiert);
   (c) Interessenvertretung (z. B. wenn eine Zertifizierungsstelle oder deren Personal zugunsten oder gegen eine bestimmte Firma agiert, die gleichzeitig ihr Kunde ist);
   (d) Übermäßige Vertrautheit, d. h. Risiken, die auf eine Zertifizierungsstelle oder deren Personal zurückzuführen sind, welche, anstatt sich um Konformitätsnachweise zu bemühen, zu vertraut oder leichtgläubig sind;
   (e) Einschüchterung (z. B. können die Zertifizierungsstelle oder deren Personal durch Risiken durch oder Angst vor einem Cloud-Anbieter oder einem anderen Beteiligten abgeschreckt werden, unparteiisch zu handeln);
   (f) Wettbewerb (z. B. zwischen dem Cloud-Anbieter und einer Vertragsperson, oder Zertifizierungsstellen am Markt).

(6) Insbesondere darf innerhalb von 24 Monaten das Personal der Zertifizierungsstelle nicht zur Bewertung von Datenverarbeitungsvorgängen oder zur Zertifizierungsentscheidung bezüglich Datenverarbeitungsvorgängen, für die es Beratung bereitgestellt hat, eingesetzt werden (s. ISO/IEC 17065:2012 Tz. 4.2.10).

(7) Es wird anerkannt, dass die Einnahmequelle der Zertifizierungsstelle die Bezahlung der Zertifizierung durch den Cloud-Anbieter ist und damit eine potentielle Gefährdung für die Unparteilichkeit gegeben ist (s. ISO/IEC 17021-1:2015 Tz. 4.2.2).

§ 3.1.3 Kompetenz

(1) Um Zertifizierungen erbringen zu können, die Vertrauen erzeugen, ist Kompetenz des Personals, unterstützt durch das Managementsystem der Zertifizierungsstelle, erforderlich (s. ISO/IEC 17065:2012 Tz. A.3).

(2) Die Zertifizierungsstelle stellt sicher, dass (ausgegliederte) Evaluatoren die notwendige Kompetenz zur Durchführung von (ausgegliederten) Tätigkeiten fortlaufend aufweisen.

§ 3.1.4 Vertraulichkeit und Offenheit

(1) Das Gleichgewicht zwischen den Zertifizierungsanforderungen, die sich auf die Vertraulichkeit und die Offenheit beziehen, hat einen Einfluss auf das Vertrauen der interessierten Parteien sowie deren Wahrnehmung über den Wert der durchgeführten Zertifizierung.

(2) Die Zertifizierungsstelle stellt sicher, dass (ausgegliederte) Evaluatoren die Tätigkeiten vertraulich durchführen.

(3) Sofern gesetzlich nicht anderweitig angeordnet, müssen insbesondere Personen, einschließlich Ausschussmitgliedern, Personal aus externen Stellen oder Personen, die im Auftrag der Zertifizierungsstelle tätig sind, alle Informationen, die sie während der Durchführung der Zertifizierungstätigkeiten erhalten oder erzeugt haben, vertraulich behandeln (s. ISO/IEC 17065:2012 Tz. 6.1.1.3).

(4) Eine Zertifizierungsstelle muss für den öffentlichen Zugang und die Offenlegung sachgemäßer und rechtzeitiger Informationen über ihre Auswahl-, Ermittlungs- und Zertifizierungsprozesse sowie über den Zertifizierungsstatus (Erteilung, Aufrechterhaltung, Erweiterung oder Einschränkung des Geltungsbereichs der Zertifizierung, Aussetzung, Widerruf oder Verweigerung der Zertifizierung) eines jeglichen Datenverarbeitungsvorgangs sorgen, um Vertrauen in die Integrität und Glaubwürdigkeit der Zertifizierung zu erzeugen (s. ISO/IEC 17065:2012 Tz. A.4.3). Offenheit ist ein Grundsatz für den Zugang zu oder die Offenlegung von entsprechenden Informationen.

§ 3.1.5 Durchführung der Zertifizierungstätigkeiten unter nicht-diskriminierenden Bedingungen

(1) Die Zertifizierungsstelle muss sicherstellen, dass grundsätzliche Regelungen und Verfahren, im Rahmen derer die Zertifizierungsstelle tätig ist, sowie ihre Verwaltung nicht-diskriminierend sind.

(2) Die Zertifizierungsstelle stellt sicher, dass Tätigkeiten durch (ausgegliederte) Evaluatoren nicht-diskriminierend durchgeführt werden.

§ 3.1.6 Abgrenzung der Verantwortlichkeiten

(1) Verantwortlich für die Erfüllung der Zertifizierungsanforderungen ist die Zertifizierungsstelle (s. ISO/IEC 17065:2012 Tz. A.6.1).

(2) Werden Tätigkeiten von ausgegliederten Evaluatoren durchgeführt, ist die Zertifizierungsstelle dafür verantwortlich, dass alle im Programm enthaltenen Zertifizierungsanforderungen von den ausgegliederten Evaluatoren erfüllt und eingehalten werden.

(3) Verantwortlich für die Erfüllung der Zertifizierungskriterien ist der Cloud-Anbieter, nicht die Zertifizierungsstelle (s. ISO/IEC 17065:2012 Tz. A.6.1).

(4) Die Zertifizierungsstelle trägt die Verantwortung dafür, ausreichend objektive Nachweise, auf denen die Zertifizierungsentscheidung basieren muss, einzuholen (s. ISO/IEC 17065:2012 Tz. A.6.2). Basierend auf einer Bewertung der Nachweise, trifft sie die Entscheidung, eine Zertifizierung zu gewähren, wenn die Konformität ausreichend nachgewiesen wird, oder eine Entscheidung, die Zertifizierung nicht zu gewähren, wenn die Konformität nicht ausreichend nachgewiesen wird.

§ 3.1.7 Offenheit für Beschwerden

(1) Interessierte Parteien erwarten, dass Beschwerden untersucht werden (s. ISO/IEC 17021-1:2015 Tz. 4.7). Falls diese für begründet befunden werden, sollten sie darauf vertrauen können, dass diese Beschwerden zweckmäßig behandelt werden und dass angemessene Anstrengungen durch die Zertifizierungsstelle zu ihrer Klärung unternommen werden. Ein tat-

sächlicher Umgang mit Beschwerden hat eine wichtige Bedeutung zum Schutz der Zertifizierungsstellen, ihrer Kunden und anderen Anwendern von Zertifizierungen vor Fehlern, Versäumnissen oder unvernünftigem Verhalten. Vertrauen in Zertifizierungstätigkeiten wird abgesichert, wenn Beschwerden entsprechend bearbeitet werden.

4 Referenzen

Beschluss Nr. 768/2008/EG	Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates (Text von Bedeutung für den EWR); http://data.europa.eu/eli/dec/2008/768(1)/oj
DAkkS 71 SD 0 001	Allgemeine Regeln zur Akkreditierung von Konformitätsbewertungsstellen. Revision: 1.3 | 29. August 2012
DAkkS 71 SD 0 013	Festlegungen für die Anwendung der DIN EN ISO/IEC 17065 bei der Akkreditierung von Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren. Revision: 1.1 | 04. Dezember 2014
DAkkS 71 SD 0 016	Regel zur Prüfung der Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme gemäß Tz. 4.6.3 EN ISO/IEC 17011. Revision: 1.3 | 27.11.2018
DSK	Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065. Version 1.0 (28.08.2018)
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. Stand 04.12.2018
Erwägungsgrund 100 zur DSGVO	Erwägungsgrund 100 Zertifizierung; https://dsgvo-gesetz.de/erwaegungsgruende/nr-100/
IAF MD 2:2017	Verbindliches Dokument für die Übertragung akkreditierter Zertifizierungen von Managementsystemen. (Deutsche Übersetzung des IAF Dokumentes „IAF MD 2:2017“); https://www.dakks.de/sites/default/files/dokumente/iaf_md_2-2017_verbindliches_dokument_fuer_die_uebertragung_akkreditierter_zertifizierungen_von_managementsystemen_uebersetzung_20190826_v1.0_0.pdf
IAF MD 4:2018	IAF MANDATORY DOCUMENT FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) FOR AUDITING/ASSESSMENT PURPOSES Issue 2. Stand 2018
IAF MD 5:2015	Ermittlung von Auditzeiten für die Auditierung von Qualitäts-management- (QMS) und Umweltmanagementsystemen (UMS). (Deutsche Übersetzung des IAF Dokumentes „IAF MD 5:2015“); https://www.dakks.de/sites/default/files/dokumente/71_sd_6_021_iaf_md_5-2015_auditzeiten_qms_ums_20160331_v1.4_0.pdf. Stand 13. März 2016
IAF MD 1:2018	Verbindliches IAF Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten (Deutsche Übersetzung des IAF Dokumentes „IAF MD 1:2018“); https://www.dakks.de/sites/default/files/dokumente/iaf_md_1-2018_auditierung_und_zertifizierung_von_managementsystemen_in_organisationen_mit_mehreren_standorten_uebersetzung_20181218_v1.0.pdf. Stand 29. Januar 2018
IAF/ILAC A5:11/2013	IAF/ILAC Multi-Lateral Mutual Recognition Arrangements (Arrangements): Application of ISO/IEC 17011:2004. Stand 2013
ISO/IEC 15408:2009	Information technology -- Security techniques -- Evaluation criteria for IT security. Stand 2009
ISO/IEC 17000:2004	Begriffe und allgemeine Grundlagen. Stand 2004.
ISO/IEC 17011:2014	Allgemeine Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen akkreditieren. Stand 2014
ISO/IEC 17020:2012	Anforderungen an den Betrieb verschiedener Typen von Stellen, die Inspektionen durchführen. Stand 2012
ISO/IEC 17021-1:2015	Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen. Stand 2015
ISO/IEC 17025:2017	Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien. Stand 2017
ISO/IEC 17030:2009	Allgemeine Anforderungen an Konformitätszeichen einer dritten Seite. Stand 2009

ISO/IEC 17065:2012	Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren. Stand 2012
ISO/IEC 17067:2013	Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme. Stand 2013
ISO/IEC 18045:2008-018	Information technology -- Security techniques -- Methodology for IT security evaluation. Stand 2008
ISO 19011:2018	Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018). Stand 2018
ISO/IEC 27006:2015	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. Stand 2015
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
Richtlinie 2013/55/EU	Richtlinie 2013/55/EU des Europäischen Parlaments und des Rates vom 20. November 2013 zur Änderung der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen und der Verordnung (EU) Nr. 1024/2012 über die Verwaltungszusammenarbeit mit Hilfe des Binnenmarkt-Informationssystems („IMI-Verordnung“) Text von Bedeutung für den EWR; http://data.europa.eu/eli/dir/2013/55/oj
Richtlinie 2006/100/EG	Richtlinie 2006/100/EG des Rates vom 20. November 2006 zur Anpassung bestimmter Richtlinien im Bereich Freizügigkeit anlässlich des Beitritts Bulgariens und Rumäniens; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32006L0100&from=HU