European Cloud Service
Data Protection Certification

AUDITOR-Konformitätsbewertungs-Programm

- Entwurfsfassung 0.4 -

Stand 05.06.2019

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Kriterienkatalog (https://doi.org/10.5445/IR/1000092273)
- 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

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

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

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

UNIKASSEL VERSITÄT

provet

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

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 Aufsichtsbehörden Zertifizierungen erteilen. Eine Zertifizierungsstelle darf ihre Tätigkeit jedoch nur aufnehmen, wenn sie durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) in Zusammenarbeit mit der zuständigen 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. DIN EN 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 Maßnahmen 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. DIN 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. Im Kapitel 2 wird der Zweck des Konformitätsbewertungsprogramm 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 die Struktur und Ressourcen der Zertifizierungsstelle. Kapitel 5 beschreibt Anforderungen an den Zertifizierungsprozess, aufgegliedert auf die Prozessphasen Auswahl, Ermittlung, Bewertung, Entscheidung, Bestätigung und Überwachung.

Bei der Spezifikation eines Konformitätsbewertungsprogramm 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.

Disclaimer

Das Konformitätsbewertungsprogramm des AUDITOR-Verfahrens ist zum aktuellen Forschungsstand nicht öffentlich einsehbar. Gemäß der aktuellen Projektplanung wird das Konformitätsbewertungsprogramm im Herbst 2019 bei der DAkkS zur Programmprüfung eingereicht. Nach Abschluss einer erfolgreichen Programmprüfung können sich Zertifizierungsstellen nach der ISO/IEC 17065 i.V.m. den ergänzenden Anforderungen zur Akkreditierung nach Art. 43 Abs. 3 DSGVO und dem AUDITOR-Programm akkreditieren lassen.

Im Folgenden sei beispielhaft das Inhaltsverzeichnis sowie ein Auszug aus einem Kapitel zur Darstellung der Inhalte des Konformitätsbewertungsprogramms dargestellt.

Inhaltsverzeichnis

3 Auszug aus dem Kapitel ‚Grundsätze'

Die Zertifizierungsstelle verpflichtet sich die Grundsätze zur Durchführung von Zertifizierungstätigkeiten einzuhalten, um das Vertrauen des Marktes in das AUDITOR-Zertifizierungsverfahren und die ausgestellten Zertifikate 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 Seite vermittelt wird.

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

§ 3.1.2 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.

§ 3.1.3 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.