

DIN ISO/IEC 19086-1

ICS 35.210

**Informationstechnik –
Cloud Computing –
Dienstgütevereinbarung (SLA) Rahmenwerk –
Teil 1: Übersicht und Konzepte (ISO/IEC 19086-1:2016)**

Information technology –
Cloud computing –
Service level agreement (SLA) framework –
Part 1: Overview and concepts (ISO/IEC 19086-1:2016)

Technologies de l'information –
Informatique en nuage –
Cadre de travail de l'accord du niveau de service –
Partie 1: Aperçu général et concepts (ISO/IEC 19086-1:2016)

Gesamtumfang 47 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich.....	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Symbole und Abkürzungen.....	14
5 Übersicht über SLA für Cloud-Dienste	14
6 Beziehung zwischen der Cloud-Dienstleistungsvereinbarung und Cloud-Dienstgütevereinbarung (Cloud-SLA).....	16
7 Bewährte Methoden des Cloud-SLA-Managements	17
7.1 Allgemeines	17
7.2 Entwurf.....	17
7.3 Beurteilung und Annahme	18
7.4 Einführung und Umsetzung	18
7.5 Änderungen an der Cloud-SLA.....	18
8 Die Funktion von Cloud-Dienstgütezielen, Qualitätszielen des Cloud-Dienstes, Metriken, Rechtsmitteln und Ausnahmen in der Cloud-SLA.....	19
8.1 Allgemeines	19
8.2 Metriken.....	19
8.3 SLO und SQO	19
8.3.1 Dienstgütern.....	19
8.3.2 Cloud-Dienstgüteziele.....	20
8.3.3 Qualitätsziele des Cloud-Dienstes	20
8.4 Rechtsmittel und Forderungen	20
8.4.1 Rechtsmittel.....	20
8.4.2 Forderungsprozess	20
8.5 Ausnahmen	21
9 Komponenten der Cloud-SLA	21
9.1 Allgemeines	21
9.2 Komponente der betroffenen Dienste	21
9.2.1 Beschreibung.....	21
9.2.2 Relevanz.....	21
9.3 Komponente der Cloud-SLA-Definitionen	22
9.3.1 Beschreibung.....	22
9.3.2 Relevanz.....	22
9.4 Komponente der Dienstüberwachung.....	22
9.4.1 Beschreibung.....	22
9.4.2 Relevanz.....	22
9.4.3 Qualitätsziele des Cloud-Dienstes	22
9.5 Komponente der Rollen und Zuständigkeiten.....	22

9.5.1	Beschreibung	22
9.5.2	Relevanz.....	22
10	Inhaltsbereiche der Cloud-SLA und ihre Komponenten	23
10.1	Allgemeines	23
10.2	Inhaltsbereich der Zugänglichkeit.....	23
10.2.1	Komponente der Zugänglichkeit	23
10.3	Inhaltsbereich der Verfügbarkeit.....	24
10.3.1	Komponente der Verfügbarkeit.....	24
10.4	Inhaltsbereich der Leistungsfähigkeit des Cloud-Dienstes	24
10.4.1	Allgemeines	24
10.4.2	Komponente der Antwortzeit des Cloud-Dienstes.....	24
10.4.3	Komponente der Kapazität des Cloud-Dienstes.....	25
10.4.4	Komponente der Elastizität.....	26
10.5	Inhaltsbereich des Schutzes personenbezogener Informationen (PII).....	27
10.5.1	Komponente des Schutzes von PII	27
10.6	Inhaltsbereich der Informationssicherheit.....	28
10.6.1	Komponente der Informationssicherheit	28
10.7	Inhaltsbereich der Kündigung des Dienstes.....	29
10.7.1	Komponente der Kündigung des Dienstes.....	29
10.8	Inhaltsbereich des Cloud-Supports.....	31
10.8.1	Komponente des Cloud-Supports.....	31
10.9	Inhaltsbereich der Governance.....	33
10.9.1	Komponente der Governance	33
10.10	Inhaltsbereich der Änderungen an den Eigenschaften und Funktionen des Cloud-Dienstes.....	35
10.10.1	Komponente der Änderungen an den Eigenschaften und Funktionen des Cloud-Dienstes	35
10.11	Inhaltsbereich der Dienstverlässlichkeit.....	35
10.11.1	Allgemeines	35
10.11.2	Komponente der Resilienz/Fehlertoleranz des Dienstes	35
10.11.3	Komponente der Sicherung und Wiederherstellung von Kundendaten.....	36
10.11.4	Komponente der Notfallwiederherstellung	38
10.12	Inhaltsbereich des Datenmanagements.....	39
10.12.1	Allgemeines	39
10.12.2	Komponente der Schutz- und Urheberrechte (IPR)	40
10.12.3	Komponente der Cloud-Kundendaten.....	40
10.12.4	Komponente der Cloud-Dienstleisterdaten.....	41
10.12.5	Komponente der Kontodaten	41
10.12.6	Komponente der abgeleiteten Daten	41
10.12.7	Komponente der Datenübertragbarkeit.....	42
10.12.8	Komponente der Datenlöschung	43
10.12.9	Komponente des Datenstandorts.....	43
10.12.10	Komponente der Datenprüfung	44
10.12.11	Komponente des Zugriffs durch Strafverfolgungsbehörden	44
10.13	Inhaltsbereich der Bescheinigungen, Zertifikate und Audits	45
10.13.1	Komponente der Bescheinigungen, Zertifikate und Audits.....	45
	Literaturhinweise.....	46

Nationales Vorwort

Diese Deutsche Norm ist die Übersetzung der Internationalen Norm ISO/IEC 19086-1:2016, die im Technischen Komitee ISO/IEC JTC 1, „Information technology“, Unterkomitee 38 „Cloud computing and distributed platforms“, in Zusammenarbeit mit ITU-T erarbeitet wurde.

Eine Liste aller Teile von ISO/IEC 19086 ist auf der ISO-Internetseite zu finden.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-01-38 AA „Verteilte Anwendungsplattformen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 9241-171:2008	siehe DIN EN ISO 9241-171:2008-10
ISO/IEC 17788:2014	siehe DIN ISO/IEC 17788:2016-04
ISO/IEC 17789	siehe DIN ISO/IEC 17789
ISO/IEC 27001	siehe DIN ISO/IEC 27001
ISO/IEC 27002	siehe DIN ISO/IEC 27002
ISO/IEC 27018	siehe DIN ISO/IEC 27018
ISO/IEC 27040	siehe DIN EN ISO/IEC 27040

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9241-171:2008-10, *Ergonomie der Mensch-System-Interaktion — Teil 171: Leitlinien für die Zugänglichkeit von Software (ISO 9241-171:2008); Deutsche Fassung EN ISO 9241-171:2008*

DIN ISO/IEC 17788:2016-04, *Informationstechnik — Cloud Computing — Übersicht und Vokabular (ISO/IEC 17788:2014)*

DIN ISO/IEC 17789, *Informationstechnik — Cloud Computing — Referenzarchitektur*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

DIN ISO/IEC 27018, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung*

DIN EN ISO/IEC 27040, *Informationstechnik — IT-Sicherheitsverfahren — Speichersicherheit*

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Die zur Erarbeitung und künftigen Revision dieses Dokumentes verwendeten Regeln sind in den ISO/IEC-Direktiven Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Regeln der ISO/IEC-Direktiven Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Einzelheiten zu Patentrechten, die während der Erarbeitung des Dokumentes identifiziert werden, werden in der Einleitung und/oder in der ISO-Liste der erhaltenen Patentdeklarationen (siehe www.iso.org/patents) angegeben.

Alle in diesem Dokument verwendeten Markennamen stellen eine Informationen für den Leser dar und stellen keine Anerkennung derselben dar.

Bezüglich einer Erklärung der Bedeutung ISO-spezifischer Ausdrücke im Zusammenhang mit Konformitätsbewertung sowie Informationen über die Einhaltung der Prinzipien der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT) seitens ISO siehe folgende URL: www.iso.org/iso/foreword.html.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, SC 38, *Cloud computing and distributed platforms* erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 19086 kann auf der ISO-Internetseite abgerufen werden.

Einleitung

Dieses Dokument liefert eine Übersicht, grundlegende Konzepte sowie Definitionen für das SLA-Rahmenwerk. ISO/IEC 19086 baut auf den in ISO/IEC 17788 und ISO/IEC 17789 definierten Konzepten des Cloud Computing auf. Dieses Dokument legt ein gemeinsames Rahmenwerk fest, das Organisationen hilft, den Zweck sämtlicher Teile von ISO/IEC 19086 sowie die Beziehungen zwischen diesen Teilen nachzuvollziehen. Zudem identifiziert es andere Dokumente, die in Beziehungen mit ISO/IEC 19086 stehen und für das Verständnis von Cloud-SLA nützlich sind.

Dieses Dokument kann von jeglicher Organisation oder Einzelperson genutzt werden, die an der Erstellung oder der Änderung einer Cloud-Dienstgütevereinbarung nach ISO/IEC 19086 beteiligt ist oder sich mit deren Inhalt befasst. Die Cloud-SLA sollte die Hauptmerkmale eines Dienstes des Cloud Computing berücksichtigen und soll ein gemeinsames Verständnis zwischen Cloud-Dienstleistern und Cloud-Dienstleistungskunden fördern.

Insbesondere definiert es die folgenden Grundlagen und Konzepte des Cloud-SLA-Rahmenwerks:

- Cloud-Dienstleistungsvereinbarung (en: Cloud Service Agreement, CSA)
- Cloud-Dienstgütevereinbarung (en: Cloud Service Level Agreement, Cloud-SLA)
- Cloud-Dienstgüteziele (en: Cloud Service Level Objectives, SLO)
- Qualitätsziele des Cloud-Dienstes (en: Cloud Service Qualitative Objectives, SQO)

Dieses Dokument beschreibt darüber hinaus die Inhaltsbereiche und Komponenten, die aus einer Liste von SLO und SQO bestehen.

- ISO/IEC 19086-2 gibt das Metrikmodell vor, das für die Erstellung von in SLO und SQO verwendeten Metriken anzuwenden ist.
- ISO/IEC 19086-3 gibt die wichtigsten Konformitätsanforderungen vor, die von den in diesem Dokument definierten SLO und SQO abgeleitet sind.
- ISO/IEC 19086-4 baut auf den in diesem Dokument beschriebenen grundlegenden Konzepten und Definitionen auf, indem sie spezifische Komponenten sowie die Konformitätsanforderungen für SLO und SQO im Bereich Sicherheit und Datenschutz beschreibt.

Im engeren Sinne dient dieses Dokument dazu,

- a) die Kohäsion zwischen den einzelnen Teilen von ISO/IEC 19086 zu fördern, indem es die in sämtlichen Teilen verwendeten Begriffe erklärt,
- b) zum Verständnis von ISO/IEC 19086 beizutragen, indem es die Beziehungen zwischen sämtlichen Teilen verdeutlicht, und
- c) eine Übersicht über andere Internationale Normen zu geben, die in Verbindung mit ISO/IEC 19086 verwendet werden kann.

Bild 1 gibt eine Übersicht über den Inhalt von ISO/IEC 19086 sowie über die Beziehungen zwischen den einzelnen Teilen von ISO/IEC 19086 und anderen Internationalen Normen mit Bezug zu Cloud Computing.

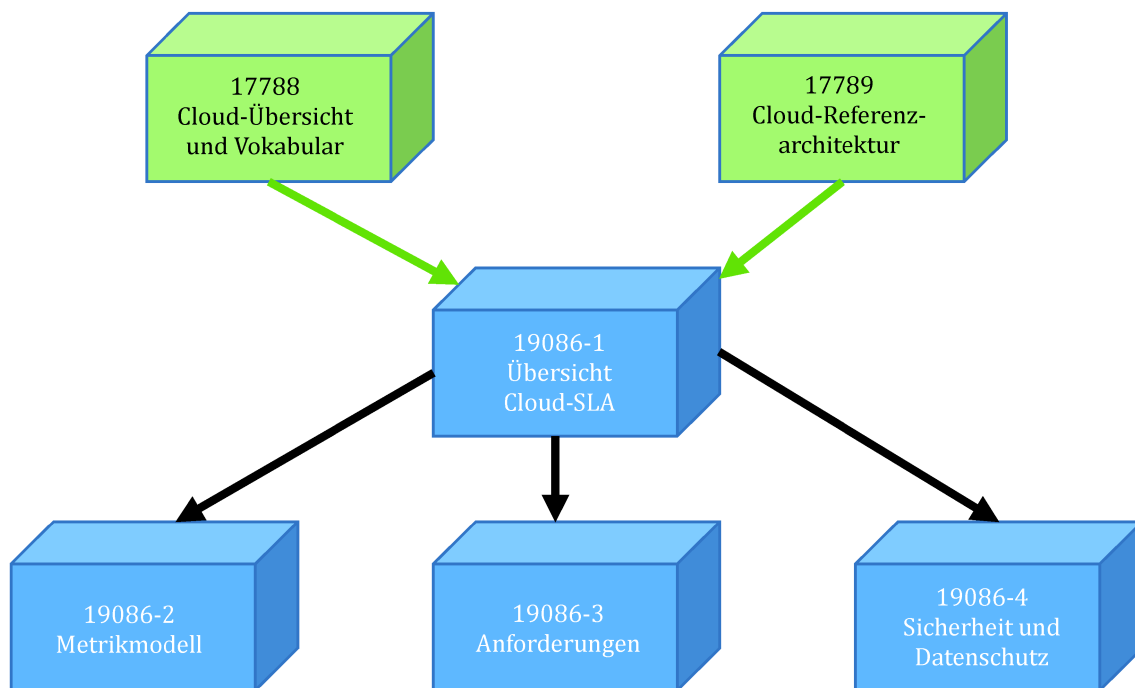


Bild 1 — Beziehung zwischen Teilen der ISO/IEC 19086 und anderen Normen zum Cloud Computing

Dieses Dokument behandelt die Inhalte einer Cloud-SLA in zwei Hauptgruppierungen: SLA-Komponenten, die in Abschnitt 9 behandelt werden, und SLA-Inhaltsbereiche, die in Abschnitt 10 behandelt werden, wie in Bild 2 dargestellt.

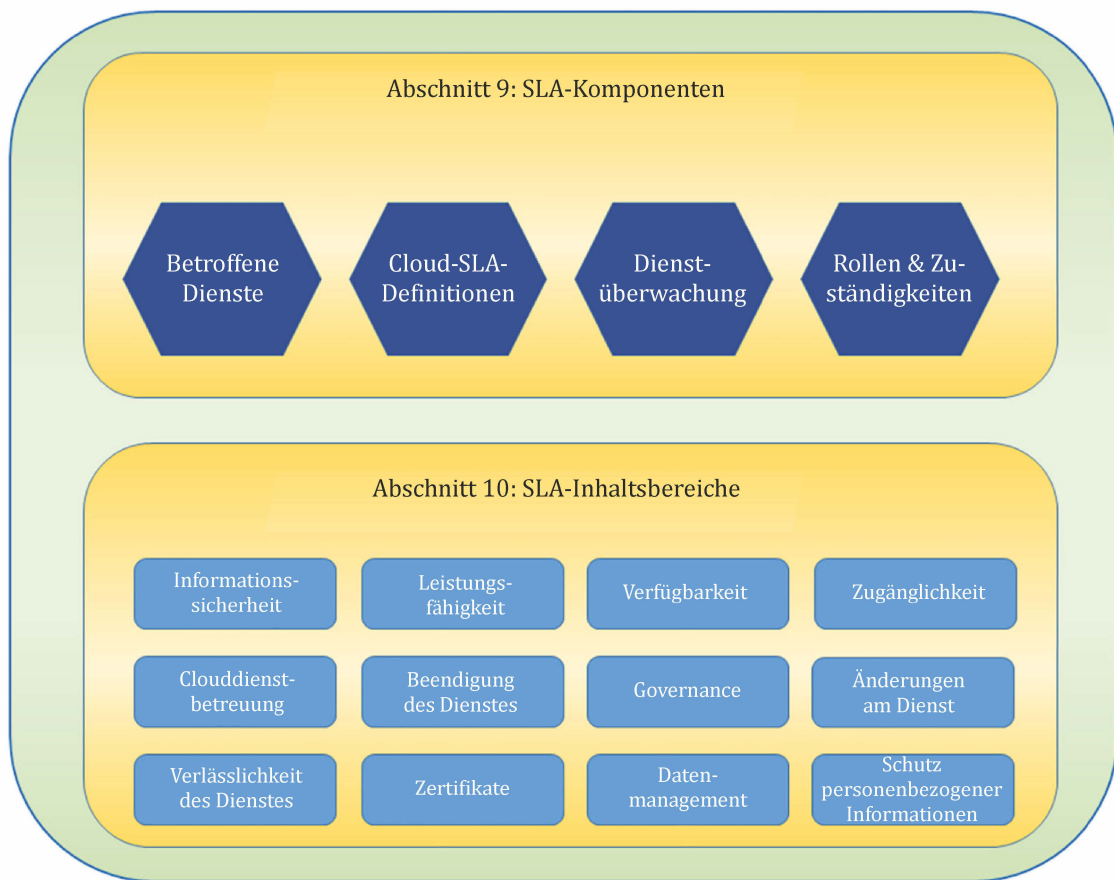


Bild 2 — SLA-Komponenten und SLA-Inhaltsbereiche

1 Anwendungsbereich

Dieses Dokument legt verschiedene gemeinsame Cloud-SLA-Bausteine (Konzepte, Begriffe, Definitionen, Kontexte) fest, die zur Erstellung von Cloud-Dienstgütevereinbarungen (Cloud-SLA) verwendet werden können.

Dieses Dokument beinhaltet Folgendes:

- a) eine Übersicht über Cloud-SLA,
- b) eine Darstellung der Beziehung zwischen der Cloud-Dienstleistungsvereinbarung und der Cloud-SLA,
- c) Konzepte, die zur Erstellung von Cloud-SLA verwendet werden können, und
- d) üblicherweise in Cloud-SLA verwendete Begriffe.

Dieses Dokument dient dem Nutzen von und der Nutzung durch Cloud-Dienstleister(n) und Cloud-Dienstleistungskunden. Ziel ist es, Verwechslungen bzw. Missverständnisse zu vermeiden sowie ein gemeinsames Verständnis zwischen Cloud-Dienstleistern und Cloud-Dienstleistungskunden zu fördern. Cloud-Dienstleistungsvereinbarungen und ihre dazugehörigen Cloud-SLA variieren je nach Cloud-Dienstleister; in manchen Fällen können verschiedene Cloud-Dienstleistungskunden für den gleichen Cloud-Dienst beim gleichen Cloud-Dienstleister unterschiedliche Vertragsbedingungen vereinbaren. Ziel dieses Dokuments ist es, Cloud-Dienstleistungskunden beim Vergleich von Cloud-Diensten verschiedener Cloud-Dienstleister zu unterstützen.

Dieses Dokument liefert keine Standardstruktur, die für eine Cloud-SLA verwendet werden kann oder eine standardmäßige Liste mit Cloud-Dienstgütezielen (SLO) und Qualitätszielen des Cloud-Dienstes (SQO), die für alle Cloud-Dienste oder alle Cloud-Dienstleister gelten würde. Dieser Ansatz bietet Cloud-Dienstleistern Flexibilität bei der individuellen Anpassung ihrer Cloud-SLA an die jeweiligen Merkmale der angebotenen Cloud-Dienste.

Dieses Dokument ersetzt keinerlei gesetzliche Bestimmungen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17788 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1

Zugänglichkeit

Gebrauchstauglichkeit eines Produkts, einer Dienstleistung, einer Umgebung oder einer Einrichtung für eine in Bezug auf ihre Fähigkeiten möglichst weit gefasste Gruppe von Menschen

Anmerkung 1 zum Begriff: Der Begriff der Zugänglichkeit betrifft den gesamten Bereich der Fähigkeiten der Benutzer und ist nicht auf Benutzer beschränkt, die formell als behindert gelten.

Anmerkung 2 zum Begriff: Der auf Gebrauchstauglichkeit ausgerichtete Begriff der Zugänglichkeit zielt darauf ab, unter Berücksichtigung der gesamten Bandbreite der Fähigkeiten, über die die einzelnen Benutzer innerhalb der Gesamtheit verfügen, ein im Hinblick auf den betreffenden Nutzungskontext möglichst hohes Ausmaß an Effektivität, Effizienz und Zufriedenstellung zu erreichen.

Anmerkung 3 zum Begriff: Im Rahmen von ISO/IEC 19086 ist es wichtig, zwischen der besonderen Bedeutung von „Zugänglichkeit“, wie hierin definiert, und dem Begriff „zugänglich“ in seiner Wörterbuchdefinition von „erreichbar oder betretbar“ zu unterscheiden.

[QUELLE: ISO 9241-171:2008, 3.2]

3.2

Aufrechterhaltung der Betriebsfähigkeit

Fähigkeit einer Organisation, die Belieferung mit Produkten oder Dienstleistungen nach einem Zwischenfall mit Betriebsunterbrechung auf akzeptablen, zuvor festgelegten Niveaustufen fortzusetzen

[QUELLE: ISO/IEC 22301:2012, 3.3]

3.3

Cloud-Dienstleistungsvereinbarung

dokumentierte Vereinbarung zwischen dem Cloud-Dienstleister und dem Cloud-Dienstleistungskunden über den/die betroffenen Dienst(e)

Anmerkung 1 zum Begriff: Eine Cloud-Dienstleistungsvereinbarung kann aus einem oder mehreren Teilen bestehen, der/die in einem oder mehreren Dokumenten festgehalten ist/sind.

3.4

Cloud-Dienstgütevereinbarung

Cloud-SLA

(en: cloud service level agreement)

Teil der Cloud-Dienstleistungsvereinbarung (3.3), der Cloud-Dienstgüteziele (3.5) sowie Qualitätsziele des Cloud-Dienstes (3.6) für den/die betroffenen Cloud-Dienst(e) beinhaltet

3.5

Cloud-Dienstgüteziel

SLO

(en: cloud service level objective)

Selbstverpflichtung eines Cloud-Dienstleisters im Hinblick auf ein bestimmtes quantitatives Merkmal eines Cloud-Dienstes, wobei der Wert der Intervallskala (3.9) oder Verhältnisskala (3.17) folgt

Anmerkung 1 zum Begriff: Eine SLO-Selbstverpflichtung darf als Bereich dargestellt werden.

3.6

Qualitätsziel des Cloud-Dienstes

SQO

(en: cloud service qualitative objective)

Selbstverpflichtung eines Cloud-Dienstleisters im Hinblick auf ein bestimmtes qualitatives Merkmal eines Cloud-Dienstes, wobei der Wert der *Nominalskala* (3.11) oder *Ordinalskala* (3.12) folgt

Anmerkung 1 zum Begriff: Ein Qualitätsziel des Cloud-Dienstes darf als Aufzählung dargestellt werden.

Anmerkung 2 zum Begriff: Qualitative Merkmale erfordern üblicherweise menschliche Interpretation.

Anmerkung 3 zum Begriff: Die Ordinalskala ermöglicht eine Einteilung in besteht/besteht nicht.

3.7

Notfallwiederherstellung

(en: disaster recovery)

Fähigkeit der IKT-Elemente einer Organisation, ihre kritischen Geschäftsfunktionen innerhalb eines vorgegebenen Zeitraums nach einem Notfall in akzeptablem Maße aufrechtzuerhalten

[QUELLE: ISO/IEC 27031:2011, 3.7]

3.8

Leitlinie zur Mitteilung von Ausfällen

(en: failure notification policy)

Leitlinie, in der die Prozesse spezifiziert werden, nach denen der Cloud-Dienstleistungskunde und der Cloud-Dienstleistungspartner den Cloud-Dienstleister über einen Dienstausfall in Kenntnis setzen können und nach denen der Cloud-Dienstleister den Cloud-Dienstleistungskunden und den Cloud-Dienstleistungspartner darüber in Kenntnis setzen kann, dass ein Dienstausfall aufgetreten ist

Anmerkung 1 zum Begriff: Die Leitlinie darf zudem den Prozess zur Bereitstellung aktueller Meldungen zu Dienstausfällen beinhalten, Angaben dazu, wer Mitteilungen und aktuelle Meldungen erhält, die größtmögliche Zeitspanne zwischen der Feststellung eines Dienstausfalls und der Herausgabe einer Mitteilung über den Dienstausfall, das größtmögliche Zeitintervall zwischen aktuellen Meldungen zu Dienstausfällen sowie Angaben dazu, wie aktuelle Meldungen zu Dienstausfällen beschrieben werden.

3.9

Intervallskala

(en: interval scale)

kontinuierliche Skala oder diskrete Skala mit äquidistanten Skalenpunkten und einem willkürlichen Nullpunkt

[QUELLE: ISO 3534-2:2006, 1.1.8]

3.10

Metrik

(en: metric)

Messstandard, der die Bedingungen und Regeln zur Durchführung der Messung und zum Verständnis der Ergebnisse einer Messung definiert

Anmerkung 1 zum Begriff: Eine Metrik setzt ein bestimmtes abstraktes Metrikkonzept um.

Anmerkung 2 zum Begriff: Eine Metrik ist in der Praxis innerhalb eines bestimmten Kontextes anzuwenden, der die Messung bestimmter Eigenschaften zu (einer) bestimmten Zeit(en) für ein bestimmtes Ziel erfordert.

3.11

Nominalskala

(en: nominal scale)

Skala mit ungeordneten gekennzeichneten Kategorien oder mit durch Übereinkunft geordneten Kategorien

[QUELLE: ISO 3534-2:2006, 1.1.6]

3.12

Ordinalskala

(en: ordinal scale)

Skala mit geordneten, gekennzeichneten Kategorien

[QUELLE: ISO 3534-2:2006, 1.1.7]

3.13

personenbezogene Informationen

PII

(en: personally identifiable information)

Informationen, die (a) dazu verwendet werden können, die betroffene Person, auf die sie sich beziehen, zu identifizieren, oder (b) direkt oder indirekt mit einem Betroffenen verknüpft sind oder verknüpft werden können

Anmerkung 1 zum Begriff: Um festzustellen, ob eine betroffene Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise vom Akteur, der die zu schützenden Daten hält, oder von einer anderen Partei angewendet werden können, um die natürliche Person zu identifizieren.

[QUELLE: ISO/IEC 29100:2011, 2.9]

3.14

PII-Beauftragter

(en: PII controller)

Datenschutz-Akteur (oder Datenschutz-Akteure), der/die die Zwecke und Mittel für die Verarbeitung der personenbezogenen Informationen (PII) festlegt/festlegen und nicht (eine) natürliche Person(en) ist/sind, die Daten für persönliche Zwecke nutzt/nutzen

[QUELLE: ISO/IEC 29100:2011, 2.10]

3.15

betroffene Person

(en: PII principal)

natürliche Person, auf die sich die personenbezogenen Informationen (PII) beziehen

[QUELLE: ISO/IEC 29100:2011, 2.11]

3.16

PII-Verarbeiter

(en: PII processor)

Datenschutz-Akteur, der personenbezogene Informationen (PII) im Auftrag eines PII-Beauftragten sowie in Übereinstimmung mit dessen Anweisungen verarbeitet

[QUELLE: ISO/IEC 29100:2011, 2.12]

3.17

Verhältnisskala

(en: ratio scale)

kontinuierliche Skala mit äquidistanten Skalenwerten und einem absoluten oder natürlichen Nullpunkt

[QUELLE: ISO 3534-2:2006, 1.1.9]

3.18

Rechtsmittel

(en: remedy)

Entschädigung, die dem Cloud-Dienstleistungskunden zur Verfügung steht, für den Fall, dass der Cloud-Dienstleister ein vorgegebenes Cloud-Dienstgüteziel (3.5) nicht erreicht

Anmerkung 1 zum Begriff: Die originalsprachliche (englische) Definition des Begriffs („remedy“) geht von der Bedeutung „legal reparation“ aus, wie sie im Wörterbuch The Shorter Oxford English Dictionary definiert ist.

3.19

Resilienz

(en: resilience)

Fähigkeit eines Cloud-Dienstes, nach Auftreten eines Fehlers zeitnah die Betriebsbedingungen wiederherzustellen

4 Symbole und Abkürzungen

BLOB	Binary Large Object (de: großes binäres Objekt)
CSA	Cloud Service Agreement (de: Cloud-Dienstleistungsvereinbarung)
CSC	Cloud Service Customer (de: Cloud-Dienstleistungskunde)
CSP	Cloud Service Provider (de: Cloud-Dienstleister)
IKT	Informations- und Kommunikationstechnik
IPR	Intellectual Property Rights (de: Schutz- und Urheberrechte)
IT	Information Technology (de: Informationstechnik)
PII	Personally Identifiable Information (de: personenbezogene Informationen)
RPO	Recovery Point Objective (de: Wiederherstellungszeitpunkt)
RTO	Recovery Time Objective (de: Wiederherstellungsdauer)
SLA	Service Level Agreement (de: Dienstgütevereinbarung)
SLO	Cloud Service Level Objective (de: Cloud-Dienstgüteziel)
SQO	Cloud Service Qualitative Objective (de: Qualitätsziel des Cloud-Dienstes)
VM	Virtual Machine (de: virtuelle Maschine)

5 Übersicht über SLA für Cloud-Dienste

Eine Cloud-Dienstgütevereinbarung (Cloud-SLA) ist ein Teil der Cloud-Dienstleistungsvereinbarung, der Cloud-Dienstgüteziele sowie Qualitätsziele des Cloud-Dienstes für den/die betroffenen Cloud-Dienst(e) beinhaltet. Die Cloud-SLA sollte die Schlüsselmerkmale des Cloud Computing nach ISO/IEC 17788:2014, 6.2, berücksichtigen, die folgende Aspekte beinhalten.

— **Anforderungsbasierte Selbstbedienung** — Ein CSC kann ohne menschliche Interaktion mit dem CSP Zugang zu Cloud-Diensten erlangen. Die Cloud-Dienstleistungsvereinbarung (CSA) (siehe Abschnitt 6) und die dazugehörige Cloud-SLA können über Software-Werkzeuge und automatisierte finanzielle Vereinbarungen vorgelegt und geschlossen werden.

- **Ressourcenreservoir** — Die öffentlichen Cloud-Bereitstellungsmodelle ermöglichen die gemeinsame Nutzung von Ressourcen durch mehrere CSC, die in keiner Beziehung zueinander stehen. Die privaten Cloud-Modelle ermöglichen Benutzern die gemeinsame Nutzung von Ressourcen innerhalb derselben Organisation. Die hybriden Cloud-Modelle ermöglichen Benutzern die gemeinsame Nutzung mancher Ressourcen innerhalb derselben Organisation und mancher Ressourcen durch mehrere CSC, die nicht notwendigerweise in einer Beziehung zueinander stehen. Die gemeinschaftlichen Cloud-Bereitstellungsmodelle ermöglichen die gemeinsame Nutzung von Ressourcen durch CSC, die in gewisser Weise in Beziehung zueinander stehen.
- **Mandantenfähigkeit** — Cloud-Umgebungen werden durch die Nutzung einer groß angelegten Virtualisierung von Servern, Speichern und Netzwerken ermöglicht. Die allgemeine Systemnutzung erfolgt üblicherweise durch viele verschiedene CSC. Mandantenfähigkeit ermöglicht die gemeinsame Nutzung von Ressourcen in einer Art und Weise, dass mehrere Mandanten und deren Rechenprozesse und Daten voneinander getrennt und füreinander unzugänglich sind. Cloud-Umgebungen verfügen üblicherweise über keinerlei permanente Beziehung zwischen bestimmten physischen Ressourcen und ihrer Nutzung durch CSC. Die CSC sind zugewiesene virtuelle Ressourcen, und die Nutzungserfassung erfolgt auf dieser Abstraktionsebene.
- **Zeitgerechte Elastizität und Skalierbarkeit** — Eine Eigenschaft des Cloud Computing, die beschreibt, wie physische oder virtuelle Ressourcen, teilweise automatisiert, schnell und elastisch angepasst werden können, um die Zuteilung von Ressourcen bedarfsgerecht schnell zu erhöhen oder zu reduzieren.
- **Kompromiss zwischen Kosten und Kontrolle** — Groß angelegte, standardisierte Cloud-Dienste können zu niedrigen Einheitskosten der Versorgung in Verbindung mit standardisierten Verträgen und Cloud-SLA bereitgestellt werden. Fordert ein CSC mehr Kontrolle und Benutzeranpassung von Cloud-Diensten als von einem Standardmodell geboten, so kann dies zu zusätzlichen Kosten und über eine spezifische Cloud-SLA bereitgestellt werden.
- **Messbarer Dienst** — Ein Merkmal, das beschreibt, dass bei der gemessenen Erbringung von Cloud-Diensten deren Nutzung überwacht, gesteuert und abgerechnet werden und eine Berichterstattung vorgenommen werden kann. Dies ist ein wichtiges Merkmal, das zur Optimierung und Validierung der erbrachten Cloud-Dienste notwendig ist. Der Fokus dieses Schlüsselmerkmals liegt auf dem Umstand, dass der CSC nur für die Ressourcen zu zahlen braucht, die er tatsächlich genutzt hat.
- **Allgemeiner Netzwerkzugang** — Die Tauglichkeiten von Cloud-Diensten werden über das Netzwerk zur Verfügung gestellt und der Zugriff auf diese erfolgt üblicherweise über Standardmechanismen, die die Verwendung heterogener Client-Plattformen (wie z. B. Zugriff über Mobiltelefone, Laptops und Arbeitsstationen) unterstützen.

Details von Cloud-SLA, SLO und SQO können für unterschiedliche Cloud-Dienstkategorien, Cloud-Tauglichkeitstypen und unterschiedliche Cloud-Bereitstellungsmodelle variieren (siehe ISO/IEC 17788). Cloud-SLA in diesem Dokument sollen für CSC und CSP über die Vielzahl von Cloud-Dienstkategorien und Cloud-Bereitstellungsmodellen hinweg nützlich sein. Da die Definitionen von SLO und SQO unabhängig von der Technologie und dem Geschäftsmodell sein sollen, gelten nicht alle dieser SLO oder SQO für jeden Cloud-Dienst, und diejenigen, die tatsächlich gelten, dürfen auf unterschiedliche Weise strukturiert und unterschiedlich auf die jeweiligen Cloud-Dienste angewendet werden. So kann z. B. die Dienstverfügbarkeit auf verschiedene Weisen gemessen werden, von denen manche vom jeweiligen Cloud-Dienst abhängen: Ein rechenintensiver Cloud-Dienst unterscheidet sich von einem E-Mail-Cloud-Dienst, weshalb die Dienstverfügbarkeit für diese unterschiedlich berechnet wird.