

DIN EN ISO/IEC 27017

ICS 03.100.70; 35.030

**Informationstechnik –
Sicherheitsverfahren –
Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend
auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015);
Deutsche Fassung EN ISO/IEC 27017:2021**

Information technology –
Security techniques –
Code of practice for information security controls based on ISO/IEC 27002 for cloud services
(ISO/IEC 27017:2015);
German version EN ISO/IEC 27017:2021

Technologies de l'information –
Techniques de sécurité –
Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002
pour les services du nuage (ISO/IEC 27017:2015);
Version allemande EN ISO/IEC 27017:2021

Gesamtumfang 55 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27017:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27017:2021 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

ISO/IEC 17788	siehe	DIN ISO/IEC 17788
ISO/IEC 17789	siehe	DIN ISO/IEC 17789
ISO 19440:2007	siehe	DIN EN ISO 19440:2009-01
ISO 31000:2009	siehe	DIN ISO 31000:2011-01
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06
ISO/IEC 27018:2014	siehe	DIN ISO/IEC 27018:2017-08
ISO/IEC 27040:2015	siehe	DIN EN ISO/IEC 27040:2017-03

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 17788, *Informationstechnik — Cloud Computing — Übersicht und Vokabular*

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

DIN EN ISO 19440:2009-01, *Unternehmensintegration — Konstrukte zur Unternehmensmodellierung (ISO 19440:2007)*; Englische Fassung EN ISO 19440:2007*

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001:2017-06, *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 27002:2017-06, *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 EN ISO/IEC 27040:2017-03, *Informationstechnik — IT-Sicherheitsverfahren — Speichersicherheit (ISO/IEC 27040:2015)*; Deutsche Fassung EN ISO/IEC 27040:2016

DIN ISO 31000:2011-01, *Risikomanagement — Grundsätze und Leitlinien (ISO 31000:2009)*

DIN ISO/IEC 27018:2017-08, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2014)*

* DIN EN ISO 19440:2009-01 wurde ersatzlos zurückgezogen.

— Leerseite —

Deutsche Fassung

Informationstechnik —
Sicherheitsverfahren —
Anwendungsleitfaden für Informationssicherheitsmaßnahmen
basierend auf ISO/IEC 27002 für Cloud Dienste
(ISO/IEC 27017:2015)

Information technology —
Security techniques —
Code of practice for information security controls
based on ISO/IEC 27002 for cloud services
(ISO/IEC 27017:2015)

Technologies de l'information —
Techniques de sécurité —
Code de pratique pour les contrôles de sécurité de
l'information fondés sur l'ISO/IEC 27002 pour les
services du nuage (ISO/IEC 27017:2015)

Diese Europäische Norm wurde vom CEN am 20. Dezember 2020 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
2.1 Identische Empfehlungen Internationale Normen	7
2.2 Zusätzliche Verweisungen	7
3 Begriffe und Abkürzungen	7
3.1 An anderer Stelle definierte Begriffe	7
3.2 Abkürzungen	8
4 Für den Cloud-Sektor spezifische Konzepte	8
4.1 Übersicht	8
4.2 Lieferantenbeziehungen bei Cloud-Diensten	9
4.3 Beziehungen zwischen Cloud-Dienstleistungskunden und Cloud-Dienstleistern	9
4.4 Umgang mit Informationssicherheitsrisiken bei Cloud-Diensten	10
4.5 Gliederung dieser Norm	10
5 Informationssicherheitsrichtlinien	11
5.1 Vorgaben der Leitung für Informationssicherheit	11
6 Organisation der Informationssicherheit	12
6.1 Interne Organisation	12
6.2 Mobilgeräte und Telearbeit	14
7 Personalsicherheit	14
7.1 Vor der Beschäftigung	14
7.2 Während der Beschäftigung	14
7.3 Beendigung und Änderung der Beschäftigung	15
8 Verwaltung der Werte	15
8.1 Verantwortlichkeit für Werte	15
8.2 Informationsklassifizierung	16
8.3 Handhabung von Datenträgern	17
9 Zugangssteuerung	17
9.1 Geschäftsanforderungen an die Zugangsteuerung	17
9.2 Benutzerzugangsverwaltung	18
9.3 Benutzerverantwortlichkeiten	20
9.4 Zugangssteuerung für Systeme und Anwendungen	20
10 Kryptographie	21
10.1 Kryptographische Maßnahmen	21
11 Physische und umgebungsbezogene Sicherheit	23
11.1 Sicherheitsbereiche	23
11.2 Geräte und Betriebsmittel	24
12 Betriebssicherheit	25
12.1 Betriebsabläufe und -verantwortlichkeiten	25

12.2	Schutz vor Schadsoftware	27
12.3	Datensicherung	27
12.4	Protokollierung und Überwachung.....	28
12.5	Steuerung von Software im Betrieb.....	30
12.6	Handhabung technischer Schwachstellen.....	30
12.7	Audit von Informationssystemen.....	31
13	Kommunikationssicherheit.....	31
13.1	Netzwerksicherheitsmanagement.....	31
13.2	Informationsübertragung	32
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	32
14.1	Sicherheitsanforderungen an Informationssysteme	32
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen.....	33
14.3	Testdaten.....	34
15	Lieferantenbeziehungen.....	34
15.1	Informationssicherheit in Lieferantenbeziehungen	34
15.2	Steuerung der Dienstleistungserbringung von Lieferanten.....	36
16	Handhabung von Informationssicherheitsvorfällen.....	36
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....	36
17	Informationssicherheitsaspekte beim Business Continuity Management	39
17.1	Aufrechterhalten der Informationssicherheit.....	39
17.2	Redundanzen	39
18	Compliance	39
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	39
18.2	Überprüfungen der Informationssicherheit	41
Anhang A Erweiterungssatz von Maßnahmen für Cloud-Dienste		43
Anhang B Verweisungen zum Informationssicherheitsrisiko im Zusammenhang mit Cloud Computing.....		49
Literaturhinweise.....		51

Europäisches Vorwort

Der Text von ISO/IEC 27017:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27017:2021 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juli 2021, und etwaige entgegenstehende nationale Normen müssen bis Juli 2021 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27017:2015 wurde von CEN als EN ISO/IEC 27017:2021 ohne irgendeine Abänderung genehmigt.

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. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe der gemeinsamen Technischen Komitees besteht in dem Erarbeiten von Internationalen Normen. Die von den gemeinsamen Technischen Komitees angenommenen Norm-Entwürfe werden den Mitgliedsorganisationen zur Umfrage zur Verfügung gestellt. Für eine Veröffentlichung als Internationale Norm wird eine Zustimmung von mindestens 75 % der Mitgliedsländer, die abgestimmt haben, benötigt.

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.

ISO/IEC 27017 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*, in Zusammenarbeit mit ITU-T erarbeitet. Der identische Text wird veröffentlicht als ITU-T. X.1631 (07/2015).

Einleitung

Die Leitlinien in dieser Empfehlung | Internationalen Norm ergänzen die Leitlinien, die in ISO/IEC 27002 enthalten sind.

Insbesondere enthält diese Empfehlung | Internationale Norm Leitlinien, die die Umsetzung der Informationssicherheitsmaßnahmen durch Cloud-Dienstleistungskunden und Cloud-Dienstleister unterstützen. Einige Leitlinien sind für Cloud-Dienstleistungskunden bestimmt, die die Maßnahmen umsetzen, und andere Leitlinien für Cloud-Dienstleister, die die Umsetzung dieser Maßnahmen unterstützen. Die Auswahl der geeigneten Informationssicherheitsmaßnahmen und die Anwendung der bereitgestellten Anleitungen zur Umsetzung hängt von der Risikobeurteilung und sämtlichen rechtlichen, vertraglichen, behördlichen oder anderen für den Cloud-Sektor spezifischen Anforderungen an die Informationssicherheit ab.

1 Anwendungsbereich

Diese Empfehlung | Internationale Norm gibt Leitfäden zu Informationssicherheitsmaßnahmen, die für die Bereitstellung und Nutzung von Cloud-Diensten anwendbar sind, durch Bereitstellung von:

- zusätzlichen Anleitungen zur Umsetzung von relevanten in ISO/IEC 27002 festgelegten Maßnahmen;
- zusätzlichen Maßnahmen mit Anleitungen zur Umsetzung, die insbesondere Cloud-Dienste betreffen.

Diese Empfehlung | Internationale Norm bietet Maßnahmen und Anleitungen zur Umsetzung sowohl für Cloud-Dienstleister als auch für Cloud-Dienstleistungskunden.

2 Normative Verweisungen

Die folgenden Empfehlungen und Internationalen Normen enthalten Festlegungen, die durch Verweisung in diesem Text Festlegungen der vorliegenden Empfehlung | Internationalen Norm sind. Zum Zeitpunkt der Veröffentlichung dieser Empfehlung | Internationalen Norm waren die angegebenen Ausgaben gültig. Alle Empfehlungen und Normen unterliegen der Überarbeitung. Vertragspartner, deren Vereinbarungen auf dieser Empfehlung | Internationalen Norm basieren, werden gebeten, die Möglichkeit zu prüfen, ob die jeweils neuesten Ausgaben der im Folgenden genannten Empfehlungen und Normen angewendet werden können. Die Mitglieder von IEC und ISO führen Verzeichnisse der gegenwärtig gültigen Internationalen Normen. Das Telecommunication Standardization Bureau der ITU pflegt eine Liste der gegenwärtig gültigen ITU-T-Empfehlungen.

2.1 Identische Empfehlungen | Internationale Normen

- ITU-T-Empfehlung Y.3500 (in Kraft) | ISO/IEC 17788: (in Kraft), *Information technology — Cloud computing — Overview and vocabulary*.
- ITU-T-Empfehlung Y.3502 (in Kraft) | ISO/IEC 17789: (in Kraft), *Information technology — Cloud computing — Reference architecture*.

2.2 Zusätzliche Verweisungen

- ISO/IEC 27000: (in Kraft), *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.
- ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*.

3 Begriffe und Abkürzungen

3.1 An anderer Stelle definierte Begriffe

Für die Anwendung dieser Empfehlung | Internationale Norm gelten die Begriffe nach ISO/IEC 27000, ITU-T-Empfehlung Y.3500 | ISO/IEC 17788, ITU-T-Empfehlung Y.3502 | ISO/IEC 17789 und die folgenden Begriffe:

3.1.1 Folgender Begriff ist in ISO 19440 definiert:

- **Fähigkeit:** Eigenschaft, in der Lage zu sein, eine bestimmte Tätigkeit auszuführen.

3.1.2 Folgende Begriffe sind in ISO/IEC 27040 definiert:

- **Bruch der Vertraulichkeit:** Beeinträchtigung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unberechtigten Offenlegung von oder den Zugang zu geschützten Daten führt, die übertragen, gespeichert oder anderweitig verarbeitet werden.

- **sichere Mandantenfähigkeit:** Art der Mandantenfähigkeit, die Sicherheitsmaßnahmen einsetzt, um ausdrücklich vor dem Bruch der Vertraulichkeit zu schützen, und die eine Validierung dieser Maßnahmen für eine ordnungsgemäße Governance vornimmt.

ANMERKUNG 1 Eine sichere Mandantenfähigkeit liegt vor, wenn das Risikoprofil eines einzelnen Mandanten nicht höher ist als es in einer zugehörigen Einzelmandantenumgebung wäre.

ANMERKUNG 2 In sehr sicheren Umgebungen wird sogar die Identität der Mandanten geheim gehalten.

3.1.3 Folgender Begriff ist in ISO/IEC 17203 definiert:

- **virtuelle Maschine:** Die vollständige Umgebung, die die Ausführung der Gastsoftware unterstützt.

ANMERKUNG Eine virtuelle Maschine ist eine Vollkapselung der virtuellen Hardware, der virtuellen Datenträger und der damit verbundenen Metadaten. Virtuelle Maschinen ermöglichen das Multiplexen der darunter liegenden physischen Maschine mittels einer Software-Schicht, dem sogenannten Hypervisor.

3.2 Abkürzungen

Für die Anwendung dieser Empfehlung | Internationalen Norm gelten die folgenden Abkürzungen:

IaaS	Infrastruktur-als-Dienst (en: Infrastructure as a Service)
PaaS	Plattform-als-Dienst (en: Platform as a Service)
pbD	personenbezogene Daten (en: personally identifiable information, PII)
SaaS	Software-als-Dienst (en: Software as a Service)
SLA	Dienstgütevereinbarung (en: Service Level Agreement)
VM	Virtuelle Maschine

4 Für den Cloud-Sektor spezifische Konzepte

4.1 Übersicht

Die Nutzung von Cloud Computing hat aufgrund der wesentlichen Änderungen in der Art und Weise, wie Rechenressourcen technisch konzipiert, betrieben und verwaltet werden, auch verändert, wie Organisationen Risiken für die Informationssicherheit beurteilen und verringern sollten. Diese Empfehlung | Internationale Norm liefert zusätzliche cloudspezifische Anleitungen zur Umsetzung auf Grundlage von ISO/IEC 27002 und legt zusätzliche Maßnahmen fest, um Überlegungen zu cloudspezifischen Bedrohungen und Risiken für die Informationssicherheit zu behandeln.

Anwender dieser Empfehlung | Internationalen Norm sollten sich hinsichtlich Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen auf ISO/IEC 27002, Abschnitt 5 bis Abschnitt 18, beziehen. Aufgrund der allgemeinen Anwendbarkeit von ISO/IEC 27002 gelten viele der Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen sowohl für den allgemeinen Kontext als auch den Kontext des Cloud Computing in einer Organisation. Beispielsweise enthält ISO/IEC 27002, 6.1.2 „Aufgabentrennung“, eine Maßnahme, die Anwendung finden kann, ungeachtet, ob die Organisation als Cloud-Dienstleister tätig ist oder nicht. Darüber hinaus kann ein Cloud-Dienstleistungskunde aus derselben Maßnahme Anforderungen für die Aufgabentrennung in der Cloud-Umgebung ableiten, z. B. indem er seine Administratoren der Cloud-Dienste von seinen Cloud-Dienstleistungsnutzern trennt.

Als Erweiterung zu ISO/IEC 27002 liefert diese Empfehlung | Internationale Norm für den Cloud-Dienst spezifische Maßnahmen, Anleitungen zur Umsetzung und sonstige Informationen (siehe 4.5), die dazu dienen, die Risiken aus den technischen und betrieblichen Eigenschaften der Cloud-Dienste zu verringern (siehe Anhang B). Die Cloud-Dienstleistungskunden und die Cloud-Dienstleister können sich auf ISO/IEC 27002 und diese Empfehlung | Internationale Norm beziehen, wenn sie Maßnahmen mit Anleitung zur Umsetzung auswählen, und bei Bedarf weitere Maßnahmen hinzufügen. Dieser Prozess kann durch Ausführen einer Informationssicherheitsrisikobeurteilung und -risikobehandlung in dem Organisations- und Geschäftskontext erfolgen, in dem Cloud-Dienste genutzt oder bereitgestellt werden (siehe 4.4).

4.2 Lieferantenbeziehungen bei Cloud-Diensten

ISO/IEC 27002, Abschnitt 15 „Lieferantenbeziehungen“, enthält Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen zur Behandlung der Informationssicherheit in Lieferantenbeziehungen. Die Bereitstellung und Nutzung von Cloud-Diensten ist eine Art Lieferantenbeziehung, in der der Cloud-Dienstleistungskunde ein Käufer und der Cloud-Dienstleister ein Lieferant ist. Aus diesem Grund gilt der Abschnitt sowohl für Cloud-Dienstleistungskunden als auch für Cloud-Dienstleister.

Cloud-Dienstleistungskunden und Cloud-Dienstleister können auch eine Lieferkette bilden. Es wird angenommen, dass ein Cloud-Dienstleister einen Dienst des Infrastrukturressourcentyps bereitstellt. Zusätzlich kann ein anderer Cloud-Dienstleister einen Dienst des Anwendungsressourcentyps bereitstellen. In diesem Fall ist der zweite Cloud-Dienstleister im Verhältnis zum ersten ein Cloud-Dienstleistungskunde und im Verhältnis zum Cloud-Dienstleistungskunden, der seinen Dienst nutzt, ein Cloud-Dienstleister. Dieses Beispiel veranschaulicht den Fall, in dem diese Empfehlung | Internationale Norm für eine Organisation sowohl als Cloud-Dienstleistungskunde als auch als Cloud-Dienstleister Anwendung findet. Da Cloud-Dienstleistungskunden und Cloud-Dienstleister durch Konzeption und Umsetzung des/der Cloud-Dienste(s) eine Lieferkette bilden, gilt ISO/IEC 27002, 15.1.3 „Lieferkette für Informations- und Kommunikationstechnologie“.

Die aus mehreren Teilen bestehende Internationale Norm ISO/IEC 27036 „*Information security for supplier relationships*“ enthält ausführliche Leitlinien zur Informationssicherheit in Lieferantenbeziehungen für Käufer und Lieferant von Produkten und Dienstleistungen.

ISO/IEC 27036 Teil 4 behandelt direkt die Sicherheit von Cloud-Diensten in Lieferantenbeziehungen. Diese Norm gilt zudem für Cloud-Dienstleistungskunden als Käufer und Cloud-Dienstleister als Lieferanten.

4.3 Beziehungen zwischen Cloud-Dienstleistungskunden und Cloud-Dienstleistern

In der Cloud-Computing-Umgebung werden die Cloud-Kundendaten von einem Cloud-Dienst gespeichert, übertragen und verarbeitet. Daher können die Geschäftsprozesse eines Cloud-Dienstleistungskunden von der Informationssicherheit des Cloud-Dienstes abhängig sein. Ohne ausreichend Kontrolle über den Cloud-Dienst hat der Cloud-Dienstleistungskunde bei seiner Informationssicherheitspraxis möglicherweise zusätzliche Vorkehrungen zu treffen.

Der Cloud-Dienstleistungskunde muss, bevor er mit einem Lieferanten eine Beziehung eingeht, bei der Auswahl des Cloud-Dienstes berücksichtigen, welche möglichen Lücken zwischen den Anforderungen an die Informationssicherheit des Cloud-Dienstleistungskunden und die Informationssicherheitsleistung des Dienstes bestehen. Wenn der Cloud-Dienst ausgewählt ist, sollte der Cloud-Dienstleistungskunde die Nutzung des Cloud-Dienstes derart verwalten, dass seine Anforderungen an die Informationssicherheit erfüllt sind. Der Cloud-Dienstleister sollte in dieser Beziehung die Informationen und den technischen Support bieten, die notwendig sind, damit die Anforderungen des Cloud-Dienstleistungskunden erfüllt werden. Wenn die Informationssicherheitsmaßnahmen des Cloud-Dienstleisters vorgegeben sind und nicht vom Cloud-Dienstleistungskunden geändert werden können, muss der Cloud-Dienstleistungskunde möglicherweise selbst zusätzliche Maßnahmen zur Risikoverringung umsetzen.

4.4 Umgang mit Informationssicherheitsrisiken bei Cloud-Diensten

Sowohl Cloud-Dienstleistungskunden als auch Cloud-Dienstleister sollten über Risikomanagementprozesse für Informationssicherheit verfügen. Ihnen wird empfohlen, die Anforderungen in ISO/IEC 27001 zur Durchführung des Risikomanagements in ihren Informationssicherheitsmanagementsystemen und weitere Anleitungen in ISO/IEC 27005 zum Informationssicherheitsrisikomanagement als solchem zu befolgen. Die Norm ISO 31000, der ISO/IEC 27001 und ISO/IEC 27005 entsprechen, kann zudem zum allgemeinen Verständnis von Risikomanagement beitragen.

Im Gegensatz zur allgemeinen Anwendbarkeit der Risikomanagementprozesse für Informationssicherheit hat das Cloud Computing eigene Risikoquellen, einschließlich Bedrohungen und Schwachstellen, die auf seine Eigenschaften zurückzuführen sind, z. B. Netzwerken, Skalierbarkeit und Elastizität des Systems, Ressourcen-Sharing, Erbringung über Selbstbedienung (Self-Service), anforderungsbasierte (On-Demand-) Administration, gerichtsbarkeitsübergreifende Dienstleistungserbringung und eingeschränkter Einblick in die Umsetzung der Maßnahmen. Anhang B enthält Verweisungen, die Angaben zu diesen Risikoquellen und zu mit der Bereitstellung und Nutzung von Cloud-Diensten verbundenen Risiken enthalten.

Die Maßnahmen und Anleitungen zur Umsetzung in Abschnitt 5 bis Abschnitt 18 und in Anhang A dieser Empfehlung | Internationalen Norm zielen auf Risikoquellen und Risiken, die für das Cloud-Computing spezifisch sind.

4.5 Gliederung dieser Norm

Diese Empfehlung | Internationale Norm ist ähnlich gegliedert wie ISO/IEC 27002. Diese Empfehlung | Internationale Norm umfasst Abschnitt 5 bis Abschnitt 18 aus ISO/IEC 27002 und gibt in jedem Abschnitt und Absatz die Anwendbarkeit der Texte an.

Wenn die in ISO/IEC 27002 festgelegten Zielsetzungen und Maßnahmen anwendbar sind, ohne dass weitere Informationen erforderlich sind, wird im vorliegenden Dokument nur auf ISO/IEC 27002 verwiesen.

Wenn eine Zielsetzung mit Maßnahmen oder eine Maßnahme unter einer Zielsetzung aus ISO/IEC 27002 zusätzlich zu jenen in ISO/IEC 27002 erforderlich ist, sind diese im normativen Anhang A „Erweiterungssatz von Maßnahmen für Cloud-Dienste“ angegeben. Wenn eine Maßnahme aus ISO/IEC 27002 oder Anhang A dieser Empfehlung | Internationalen Norm eine zusätzliche cloudspezifische Anleitung zur Umsetzung in Bezug auf die Maßnahme benötigt, ist diese unter dem Untertitel „**Anleitung zur Umsetzung für Cloud-Dienste**“ aufgeführt. Die Anleitungen werden in Form einer der beiden folgenden Typen gegeben:

Typ 1 wird verwendet, wenn es eine separate Anleitung für den Cloud-Dienstleistungskunden und den Cloud-Dienstleister gibt.

Typ 2 wird verwendet, wenn die Anleitung für den Cloud-Dienstleistungskunden und den Cloud-Dienstleister identisch ist.

Typ 1

Cloud-Dienstleistungskunde	Cloud-Dienstleister

Typ 2

Cloud-Dienstleistungskunde	Cloud-Dienstleister

Weitere Informationen, die möglicherweise zu berücksichtigen sind, werden unter dem Untertitel „**Weitere Informationen für Cloud-Dienste**“ aufgeführt.

5 Informationssicherheitsrichtlinien

5.1 Vorgaben der Leitung für Informationssicherheit

Es gilt das Ziel von ISO/IEC 27002, 5.1.

5.1.1 Informationssicherheitsrichtlinien

Es gelten die Maßnahme 5.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung zur Umsetzung für Cloud-Dienste

Cloud-Dienstleistungskunde	Cloud-Dienstleister
<p>Eine Informationssicherheitsrichtlinie für Cloud Computing sollte als themenspezifische Richtlinie des Cloud-Dienstleistungskunden festgelegt werden. Die Informationssicherheitsrichtlinie für Cloud Computing des Cloud-Dienstleistungskunden sollte mit den für die Organisation annehmbaren Grenzen der Informationssicherheitsrisiken für ihre Informationen und anderen Werte konsistent sein.</p> <p>Bei der Erstellung der Informationssicherheitsrichtlinie für Cloud Computing sollte der Cloud-Dienstleistungskunde Folgendes berücksichtigen:</p> <ul style="list-style-type: none"> — in der Cloud-Computing-Umgebung gespeicherte Informationen können dem Zugang und der Verwaltung des Cloud-Dienstleisters unterliegen; — Werte können in der Cloud-Computing-Umgebung gepflegt werden, z. B. Anwendungsprogramme; — Prozesse können auf einem mandantenfähigen, virtualisierten Cloud-Dienst laufen; — die Cloud-Dienstleistungsnutzer und der Kontext, in dem sie den Cloud-Dienst verwenden; — die Administratoren des Cloud-Dienstes beim Cloud-Dienstleistungskunden, die privilegierten Zugang haben; — die geographischen Standorte der Organisation des Cloud-Dienstleisters und die Länder, in denen der Cloud-Dienstleister die Cloud-Kundendaten (auch temporär) speichern kann. 	<p>Der Cloud-Dienstleister sollte seine Informationssicherheitsrichtlinie ergänzen und die Bereitstellung und Nutzung seiner Cloud-Dienste darin aufnehmen, und dabei Folgendes berücksichtigen:</p> <ul style="list-style-type: none"> — die grundlegenden Anforderungen an die Informationssicherheit, die auf die Konzeption und Umsetzung des Cloud-Dienstes anwendbar sind; — Risiken durch Insider mit Berechtigungen; — Mandantenfähigkeit und Isolation des Cloud-Dienstleistungskunden (einschließlich Virtualisierung); — Zugang zu den Werten des Cloud-Dienstleistungskunden durch Mitarbeiter des Cloud-Dienstleisters; — Verfahren zur Zugriffskontrolle, z. B. starke Authentifizierung für administrativen Zugriff auf die Cloud-Dienste; — Kommunikation mit dem Cloud-Dienstleistungskunden während des Änderungsmanagements; — Virtualisierungssicherheit; — Zugriff auf und Schutz der Cloud-Kundendaten; — Lebenszyklusmanagement der Konten des Cloud-Dienstleistungskunden; — Kommunikation von Brüchen der Vertraulichkeit und Leitfäden zum Informationsaustausch, um Untersuchungen und Forensik zu unterstützen.

Sonstige Informationen für Cloud-Dienste

Die Informationssicherheitsrichtlinie für Cloud Computing des Cloud-Dienstleistungskunden ist eine der themenspezifischen Richtlinien, die in ISO/IEC 27002, 5.1.1 beschrieben werden. Die Informationssicherheitsrichtlinie einer Organisation behandelt deren Informationen und Geschäftsprozesse. Verwendet

eine Organisation Cloud-Dienste, kann sie eine Richtlinie für Cloud Computing als Cloud-Dienstleistungskunde haben. Die Informationen einer Organisation können in der Cloud-Computing-Umgebung gespeichert und gepflegt werden, und die Geschäftsprozesse können in der Cloud-Computing-Umgebung ablaufen. Allgemeine Anforderungen an die Informationssicherheit, die in der Informationssicherheitsrichtlinie auf höchster Ebene festgelegt sind, werden in die Richtlinie für Cloud Computing übernommen.

Im Unterschied hierzu behandelt die Informationssicherheitsrichtlinie zur Bereitstellung von Cloud-Diensten die Informationen und Geschäftsprozesse des Cloud-Dienstleistungskunden und nicht die Informationen und Geschäftsprozesse des Cloud-Dienstleisters. Die Anforderungen an die Informationssicherheit für die Bereitstellung des Cloud-Dienstes sollten denen der potentiellen Cloud-Dienstleistungskunden entsprechen. Hierdurch könnten sie nicht mit den Anforderungen an die Informationssicherheit für die Informationen und Geschäftsprozesse des Cloud-Dienstleisters übereinstimmen. Der Anwendungsbereich der Informationssicherheitsrichtlinie wird oft im Hinblick auf den Dienst, aber nicht ausschließlich durch die Organisationsstruktur oder die physischen Standorte festgelegt.

Beim Cloud Computing sind verschiedene Virtualisierungssicherheitsaspekte zu beachten, darunter das Lebenszyklusmanagement virtueller Instanzen, Speicher- und Zugangssteuerung für virtualisierte Images, Umgang mit virtuellen Instanzen im Ruhe- oder Offline-Zustand, Speicherauszüge, Schutz der Hypervisoren und Sicherheitsmaßnahmen zur Regelung der Nutzung der Self-Service-Portale.

5.1.2 Überprüfung der Informationssicherheitsrichtlinien

Es gelten die Maßnahme 5.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Es gilt das Ziel von ISO/IEC 27002, 6.1.

6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Es gelten die Maßnahme 6.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung zur Umsetzung für Cloud-Dienste

Cloud-Dienstleistungskunde	Cloud-Dienstleister
<p>Der Cloud-Dienstleistungskunde sollte mit dem Cloud-Dienstleister eine angemessene Zuweisung der Informationssicherheitsrollen und -verantwortlichkeiten vereinbaren und bestätigen, dass er die ihm zugeteilten Rollen und Verantwortlichkeiten erfüllen kann. Die Informationssicherheitsrollen und -verantwortlichkeiten beider Parteien sollten in einer Vereinbarung dokumentiert werden.</p> <p>Der Cloud-Dienstleistungskunde sollte seine Beziehung mit dem Kundendienst beim Cloud-Dienstleister identifizieren und verwalten.</p>	<p>Der Cloud-Dienstleister sollte eine angemessene Zuweisung der Informationssicherheitsrollen und -verantwortlichkeiten mit seinen Cloud-Dienstleistungskunden, seinen Cloud-Dienstleistern und seinen Lieferanten vereinbaren und dokumentieren.</p>

Sonstige Informationen für Cloud-Dienste

Auch wenn die Parteien unter sich die Verantwortlichkeiten festlegen, ist der Cloud-Dienstleistungskunde für die Entscheidung, den Dienst zu nutzen, verantwortlich. Diese Entscheidung sollte entsprechend den in der Organisation des Cloud-Dienstleistungskunden festgelegten Rollen und Verantwortlichkeiten gefällt werden. Der Cloud-Dienstleister ist für die Informationssicherheit verantwortlich, die als Teil der Cloud-Dienstleistungsvereinbarung beschlossen wurde. Die Umsetzung und Bereitstellung von Informationssicherheit sollte entsprechend den in der Organisation des Cloud-Dienstleisters festgelegten Rollen und Verantwortlichkeiten erfolgen.

Unklare Rollen und eine missverständliche Definition und Zuteilung der Verantwortlichkeiten in Bezug auf Themen wie Dateneigentum, Zugangssteuerung und Wartung der Infrastruktur, können zu Geschäfts- oder Rechtsstreitigkeiten führen, insbesondere wenn Dritte beteiligt sind.

Daten und Dateien auf den Systemen des Cloud-Dienstleisters, die während der Nutzung des Cloud-Dienstes erstellt oder geändert werden, können für den sicheren Betrieb, die Wiederherstellung und die Aufrechterhaltung des Dienstes kritisch sein. Die Zuständigkeiten für alle Werte sowie die Parteien, die Verantwortlichkeiten hinsichtlich Vorgängen, wie Sicherungs- und Wiederherstellungsvorgängen, in Bezug auf diese Werte haben, sollten festgelegt und dokumentiert werden. Ansonsten besteht das Risiko, dass der Cloud-Dienstleister davon ausgeht, dass der Cloud-Dienstleistungskunde diese entscheidenden Aufgaben übernimmt (oder umgekehrt), und es kann zu einem Datenverlust kommen.

6.1.2 Aufgabentrennung

Es gelten die Maßnahme 6.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6.1.3 Kontakt mit Behörden

Es gelten die Maßnahme 6.1.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung zur Umsetzung für Cloud-Dienste

Cloud-Dienstleistungskunde	Cloud-Dienstleister
Der Cloud-Dienstleistungskunde sollte die Behörden, die für gemeinsame Vorgänge des Cloud-Dienstleistungskunden und des Cloud-Dienstleisters zuständig sind, identifizieren.	Der Cloud-Dienstleister sollte den Cloud-Dienstleistungskunden über die geographischen Standorte der Organisation des Cloud-Dienstleisters und die Länder, in denen der Cloud-Dienstleister die Cloud-Kundendaten speichern kann, informieren.

Sonstige Informationen für Cloud-Dienste

Informationen über geographische Standorte, an denen die Cloud-Kundendaten gespeichert, verarbeitet und übertragen werden können, können dem Cloud-Dienstleistungskunden dabei behilflich sein, die Aufsichtsbehörden und Gerichtsbarkeiten zu bestimmen.

6.1.4 Kontakt mit speziellen Interessensgruppen

Es gelten die Maßnahme 6.1.4 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.