

DIN EN ISO/IEC 27017



ICS 03.100.70; 35.030

Einsprüche bis 2020-10-21

Entwurf

**Informationstechnik –
Sicherheitsverfahren –
Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend
auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015);
Deutsche und Englische Fassung prEN ISO/IEC 27017:2020**

Information technology –
Security techniques –
Code of practice for information security controls based on ISO/IEC 27002 for cloud services
(ISO/IEC 27017:2015);
German and English version prEN ISO/IEC 27017:2020

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 et anglaise prEN ISO/IEC 27017:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-08-21 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im
Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-
Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 96 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 prEN ISO/IEC 27017:2020 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO 19440:2007	siehe	DIN EN ISO 19440:2009-01
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2013	siehe	E DIN EN ISO/IEC 27001:2017-12
ISO/IEC 27002:2013	siehe	E DIN EN ISO/IEC 27002:2017-12
ISO/IEC 27018:2014	siehe	DIN EN ISO/IEC 27002:2020-08
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 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*

E DIN EN ISO/IEC 27001:2017-12, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)*; Deutsche Fassung EN ISO/IEC 27001:2017

E DIN EN ISO/IEC 27002:2017-12, *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 27002:2020-08, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2019)*; Deutsche Fassung EN ISO/IEC 27018:2020

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

— Leerseite —

<i>Titel de:</i>	Informationstechnik — Sicherheitsverfahren — Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015)
<i>Titel en:</i>	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)
<i>Titel fr:</i>	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)

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 Begriffe	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) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27017:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27017:2015 wurde von CEN als prEN ISO/IEC 27017:2020 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 enthält Leitlinien zu Informationssicherheitsmaßnahmen, die für die Bereitstellung und Nutzung von Cloud-Diensten gelten, darunter:

- zusätzliche Anleitungen zur Umsetzung von relevanten in ISO/IEC 27002 festgelegten Maßnahmen;
- zusätzliche 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 Bestandteil 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:

- **Kapazität:** 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, 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 Begriffe

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 cloudbezogenen Bedrohungen und Risiken für die Informationssicherheit zu behandeln.

Anwender dieser Empfehlung | Internationalen Norm sollten sich hinsichtlich Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen auf die Abschnitte 5 bis 18 in ISO/IEC 27002 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 6.1.2 „Aufgabentrennung“ in ISO/IEC 27002 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 oder 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

Abschnitt 15 „Lieferantenbeziehungen“ in ISO/IEC 27002 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 Infrastrukturauglichkeitstyps bereitstellt. Zusätzlich kann ein anderer Cloud-Dienstleister einen Dienst des Anwendungstauglichkeitstyps 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 15.1.3 „Lieferkette für Informations- und Kommunikationstechnologie“ in ISO/IEC 27002.

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.

Teil 4 der ISO/IEC 27036 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 kann der Geschäftsprozess eines Cloud-Dienstleistungskunden von der Informationssicherheit des Cloud-Dienstes abhängig sein. Ohne ausreichend Kontrolle über den Cloud-Dienst muss der Cloud-Dienstleistungskunde bei seiner Informationssicherheitspraxis möglicherweise zusätzliche Vorkehrungen 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 den Informationssicherheitskapazitäten 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 Risikoverringerung 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 selbst zu befolgen. Die Norm ISO 31000, mit der ISO/IEC 27001 und ISO/IEC 27005 übereinstimmen, 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, rechtsgebietsübergreifende 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 den Abschnitten 5 bis 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 beinhaltet die Abschnitte 5 bis 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 den Cloud-Dienst“ 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>Als themenspezifische Richtlinie des Cloud-Dienstleistungskunden sollte eine Informationssicherheitsrichtlinie für Cloud Computing festgelegt werden. Die Informationssicherheitsrichtlinie für Cloud Computing des Cloud-Dienstleistungskunden sollte mit den für die Organisation annehmbaren Grenzen der Informationssicherheitsrisiken für ihre Informationen und 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 der Cloud-Dienst verwendet wird;— die Administratoren des Cloud-Dienstes beim Cloud-Dienstleistungskunden, die privilegierten Zugang haben;— die geografischen 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 behandelt 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 Informations-sicherheitsrichtlinie auf höchster Ebene festgelegt sind, werden in die Richtlinie für Cloud Computing übernommen.

Die Informationssicherheitsrichtlinie zur Bereitstellung von Cloud-Diensten behandelt jedoch 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 potenziellen Cloud-Dienstleistungskunden entsprechen. Demnach 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 Bilder, Umgang mit virtuellen Instanzen im Ruhe- oder Offline-Zustand, Speicherauszüge, Schutz der Hypervisoren und Sicherheitsmaßnahmen zur Regelung Nutzung der 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 Zuteilung 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 und dem für die Betreuung Verantwortlichen beim Cloud-Dienstleister identifizieren und verwalten.</p>	<p>Der Cloud-Dienstleister sollte eine angemessene Zuteilung 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. Das Eigentum aller Werte sowie die Parteien, die Verantwortlichkeiten hinsichtlich Vorgängen, wie Sicherungs- und Wiederherstellungsvorgängen, mit diesen Werten 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 geografischen 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 geografische Standorte, an denen die Cloud-Kundendaten gespeichert, verarbeitet und übertragen werden können, können dem Cloud-Dienstleistungskunden dabei behilflich sein, die Aufsichtsbehörden und Gerichtbarkeiten 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.

6.1.5 Informationssicherheit im Projektmanagement

Es gelten die Maßnahme 6.1.5 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6.2 Mobilgeräte und Telearbeit

Es gilt das Ziel von ISO/IEC 27002, 6.2.

6.2.1 Richtlinie zu Mobilgeräten

Es gelten die Maßnahme 6.2.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6.2.2 Telearbeit

Es gelten die Maßnahme 6.2.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7 Personalsicherheit

7.1 Vor der Beschäftigung

Es gilt das Ziel von ISO/IEC 27002, 7.1.

7.1.1 Sicherheitsüberprüfung

Es gelten die Maßnahme 7.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Es gelten die Maßnahme 7.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7.2 Während der Beschäftigung

Es gilt das Ziel von ISO/IEC 27002, 7.2.

7.2.1 Verantwortlichkeiten der Leitung

Es gelten die Maßnahme 7.2.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Es gelten die Maßnahme 7.2.2 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 die folgenden Punkte in seine Bewusstseins-, Ausbildungs- und Schulungsprogramme für Geschäftsführer, Administratoren, Integratoren und Benutzer von Cloud-Diensten, einschließlich der betreffenden Mitarbeiter und Auftragnehmer, aufnehmen:</p> <ul style="list-style-type: none">— Normen und Verfahren für die Nutzung von Cloud-Diensten;— Informationssicherheitsrisiken im Bezug auf Cloud-Dienste und wie diesen Risiken begegnet wird;— Risiken für System- und Netzwerkumgebungen bei der Nutzung von Cloud-Diensten;— geltende gesetzliche und behördliche Überlegungen. <p>Programme zu Informationssicherheitsbewusstsein, -ausbildung und -schulung bei Cloud-Diensten sollten der Unternehmensleitung und Mitarbeitern in Führungspositionen, einschließlich der Leitung von Geschäftseinheiten, angeboten werden. Diese Bestrebungen tragen zu einer effektiven Koordination der Tätigkeiten im Bereich der Informationssicherheit bei.</p>	<p>Der Cloud-Dienstleister sollte hinsichtlich der angemessenen Handhabung von Cloud-Kundendaten und abgeleiteten Cloud-Dienstleistungsdaten bei seinen Mitarbeitern Bewusstsein schaffen und Ausbildung und Schulung anbieten; dasselbe sollte er von seinen Auftragnehmern fordern. Diese Daten können vertrauliche Informationen der Cloud-Dienstleistungskunden enthalten oder bestimmten (auch behördlichen) Einschränkungen im Bezug auf Zugang und Nutzung durch den Cloud-Dienstleister unterliegen.</p>

7.2.3 Maßregelungsprozess

Es gelten die Maßnahme 7.2.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7.3 Beendigung und Änderung der Beschäftigung

Es gilt das Ziel von ISO/IEC 27002, 7.3.

7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Es gelten die Maßnahme 7.3.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8 Verwaltung der Werte

8.1 Verantwortlichkeit für Werte

Es gilt das Ziel von ISO/IEC 27002, 8.1.

8.1.1 Inventarisierung der Werte

Es gelten die Maßnahme 8.1.1 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
Die Inventarisierung der Werte des Cloud-Dienstleistungskunden sollte die Informationen und damit verbundenen Werte berücksichtigen, die in der Cloud-Computing-Umgebung gespeichert sind. Die Aufzeichnungen des Inventars sollten angeben, wo die Werte gepflegt werden, z. B. Identifizierung des Cloud-Dienstes.	Die Inventarisierung der Werte durch den Cloud-Dienstleister sollte Folgendes explizit identifizieren: <ul style="list-style-type: none">— Cloud-Kundendaten;— abgeleitete Cloud-Dienstleistungsdaten.

Sonstige Informationen für Cloud-Dienste

Es gibt Anwendungen für Cloud-Dienste, die Funktionen bieten, Informationen zu verwalten, indem abgeleitete Cloud-Dienstleistungsdaten zu den Cloud-Kundendaten hinzugefügt werden. Wenn diese abgeleiteten Cloud-Dienstleistungsdaten als Werte identifiziert und diese im Inventar der Werte geführt werden, kann dies zur Verbesserung der Informationssicherheit beitragen.

8.1.2 Zuständigkeit für Werte

Es gelten die Maßnahme 8.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

Sonstige Informationen für Cloud-Dienste

Die Zuständigkeit für Werte variiert wahrscheinlich abhängig von der Kategorie des genutzten Cloud-Dienstes. Anwendungssoftware ist Eigentum des Cloud-Dienstleistungskunden, wenn er eine Plattform-als-Dienst (PaaS) oder eine Infrastruktur-als-Dienst (IaaS) nutzt. Wenn er hingegen eine Software-als-Dienst (SaaS) nutzt, ist die Anwendungssoftware Eigentum des Cloud-Dienstleisters.

8.1.3 Zulässiger Gebrauch von Werten

Es gelten die Maßnahme 8.1.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8.1.4 Rückgabe von Werten

Es gelten die Maßnahme 8.1.4 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8.2 Informationsklassifizierung

Es gilt das Ziel von ISO/IEC 27002, 8.2.

8.2.1 Klassifizierung von Information

Es gelten die Maßnahme 8.2.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8.2.2 Kennzeichnung von Information

Es gelten die Maßnahme 8.2.2 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 Informationen und zugehörige Werte, die in der Cloud-Computing-Umgebung gepflegt werden, in Übereinstimmung mit den Verfahren zur Kennzeichnung des Cloud-Dienstleistungskunden kennzeichnen. Gegebenenfalls können die Funktionen, die der Cloud-Dienstleister bereitstellt und das Kennzeichnen unterstützen, verwendet werden.	Der Cloud-Dienstleister sollte jede Funktion des Dienstes, die er bereitstellt und die dem Cloud-Dienstleistungskunden ermöglicht, seine Informationen und zugehörigen Werte zu klassifizieren und zu kennzeichnen, dokumentieren und offenlegen.

8.2.3 Handhabung von Werten

Es gelten die Maßnahme 8.2.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8.3 Handhabung von Datenträgern

Es gilt das Ziel von ISO/IEC 27002, 8.3.

8.3.1 Handhabung von Wechseldatenträgern

Es gelten die Maßnahme 8.3.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8.3.2 Entsorgung von Datenträgern

Es gelten die Maßnahme 8.3.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

8.3.3 Transport von Datenträgern

Es gelten die Maßnahme 8.3.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9 Zugangssteuerung

9.1 Geschäftsanforderungen an die Zugangsteuerung

Es gilt das Ziel von ISO/IEC 27002, 9.1.

9.1.1 Zugangssteuerungsrichtlinie

Es gelten die Maßnahme 9.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Es gelten die Maßnahme 9.1.2 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
Die Zugangssteuerungsrichtlinie des Cloud-Dienstleistungskunden für die Nutzung von Netzwerken und Netzwerkdiensten sollte die Anforderungen an den Benutzerzugang für jeden einzelnen genutzten Cloud-Dienst festlegen.	(keine weitere Anleitung zur Umsetzung)

9.2 Benutzerzugangsverwaltung

Es gilt das Ziel von ISO/IEC 27002, 9.2.

9.2.1 Registrierung und Deregistrierung von Benutzern

Es gelten die Maßnahme 9.2.1 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
(keine weitere Anleitung zur Umsetzung)	Um den Zugang zu Cloud-Diensten durch einen Cloud-Dienstleistungsnutzer des Cloud-Dienstleistungskunden zu verwalten, sollte der Cloud-Dienstleister dem Cloud-Dienstleistungskunden Funktionen für die Registrierung und Deregistrierung von Benutzern sowie Spezifikationen, wie diese Funktionen zu verwenden sind, bereitstellen.

9.2.2 Zuteilung von Benutzerzugängen

Es gelten die Maßnahme 9.2.2 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
(keine weitere Anleitung zur Umsetzung)	Der Cloud-Dienstleister sollte Funktionen zur Verwaltung der Zugangsrechte der Cloud-Dienstleistungsnutzer des Cloud-Dienstleistungskunden sowie Spezifikationen, wie diese Funktionen zu verwenden sind, anbieten.

Sonstige Informationen für Cloud-Dienste

Der Cloud-Dienstleister sollte die Technologien zur Identitäts- und Zugangsverwaltung Dritter für seine Cloud-Dienste und die zugehörigen Administrationsschnittstellen unterstützen. Diese Technologien können die Integration und Verwaltung der Benutzeridentitäten zwischen den Systemen des Cloud-

Dienstleistungskunden und dem Cloud-Dienst sowie die Nutzung mehrerer Cloud-Dienste vereinfachen, indem diese Kapazitäten als Single Sign-on (Einmalanmeldung) unterstützt werden.

9.2.3 Verwaltung privilegierter Zugangsrechte

Es gelten die Maßnahme 9.2.3 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 für die administrativen Kapazitäten eines Cloud-Dienstes entsprechend den ermittelten Risiken ausreichende Authentifizierungstechniken (z. B. Multifaktor-Authentifizierung) für die Authentifizierung der Administratoren des Cloud-Dienstes seitens des Cloud-Dienstleistungskunden verwenden.	Der Cloud-Dienstleister sollte für die administrativen Kapazitäten eines Cloud-Dienstes entsprechend den ermittelten Risiken ausreichende Authentifizierungstechniken für die Authentifizierung der Administratoren des Cloud-Dienstes seitens des Cloud-Dienstleistungskunden zur Verfügung stellen. Der Cloud-Dienstleister kann beispielsweise Kapazitäten der Multifaktor-Authentifizierung bereitstellen oder die Nutzung von Mechanismen zur Multifaktor-Authentifizierung Dritter ermöglichen.

9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern

Es gelten die Maßnahme 9.2.4 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 verifizieren, dass die Verwaltungsverfahren für die Zuteilung geheimer Authentisierungsdaten, wie Passwörter, den Anforderungen des Cloud-Dienstleistungskunden entsprechen.	Der Cloud-Dienstleister sollte Informationen über Verfahren zur Verwaltung der geheimen Authentisierungsdaten der Cloud-Dienstleistungskunden zur Verfügung stellen, einschließlich Verfahren für die Zuteilung dieser Informationen sowie für die Benutzerauthentisierung.

Sonstige Informationen für Cloud-Dienste

Der Cloud-Dienstleistungskunde sollte die Verwaltung der geheimen Authentisierungsdaten steuern, indem er eigene Technologien zur Identitäts- und Zugangsverwaltung oder solche Technologien Dritter nutzt.

9.2.5 Überprüfung von Benutzerzugangsrechten

Es gelten die Maßnahme 9.2.5 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.2.6 Entzug oder Anpassung von Zugangsrechten

Es gelten die Maßnahme 9.2.6 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.3 Benutzerverantwortlichkeiten

Es gilt das Ziel von ISO/IEC 27002, 9.3.

9.3.1 Gebrauch geheimer Authentisierungsinformation

Es gelten die Maßnahme 9.3.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.4 Zugangssteuerung für Systeme und Anwendungen

Es gilt das Ziel von ISO/IEC 27002, 9.4.

9.4.1 Informationszugangsbeschränkung

Es gelten die Maßnahme 9.4.1 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
Der Cloud-Dienstleistungskunde sollte sicherstellen, dass der Zugang zu Informationen im Cloud-Dienst in Übereinstimmung mit der Zugangssteuerungsrichtlinie eingeschränkt werden kann und dass diese Einschränkungen umgesetzt werden. Dazu zählen auch Einschränkungen des Zugangs zu Cloud-Diensten, zu Funktionen des Cloud-Dienstes und zu Cloud-Kundendaten, die im Dienst geführt werden.	Der Cloud-Dienstleister sollte Zugangssteuerungen bereitstellen, die es dem Cloud-Dienstleistungskunden ermöglichen, den Zugang zu Cloud-Diensten, zu Funktionen des Cloud-Dienstes und zu Cloud-Kundendaten, die im Dienst geführt werden, zu beschränken.

Sonstige Informationen für Cloud-Dienste

Die Cloud-Computing-Umgebung umfasst zusätzliche Bereiche, die Zugangssteuerung erfordern. Als Teil des Cloud-Dienstes oder der Funktionen des Cloud-Dienstes muss der Zugang zu Funktionen und Diensten, wie die Managementfunktionen des Hypervisors und Administratorkonsolen, möglicherweise über eine zusätzliche Zugangssteuerung verfügen.

9.4.2 Sichere Anmeldeverfahren

Es gelten die Maßnahme 9.4.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.4.3 System zur Verwaltung von Kennwörtern

Es gelten die Maßnahme 9.4.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Es gelten die Maßnahme 9.4.4 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
Wo der Gebrauch von Hilfsprogrammen zulässig ist, sollte der Cloud-Dienstleistungskunde die Hilfsprogramme identifizieren, die in seiner Cloud-Computing-Umgebung verwendet werden sollen, und sicherstellen, dass diese nicht die Maßnahmen des Cloud-Dienstes beeinträchtigen.	Der Cloud-Dienstleister sollte die Anforderungen an alle Hilfsprogramme identifizieren, die innerhalb des Cloud-Dienstes verwendet werden. Der Cloud-Dienstleister sollte sicherstellen, dass jeder Gebrauch von Hilfsprogrammen, die in der Lage sind, übliche Betriebs- und Sicherheitsverfahren zu umgehen, streng auf befugtes Personal beschränkt ist, und dass der Gebrauch dieser Programme regelmäßig geprüft und auditiert wird.

9.4.5 Zugangssteuerung für Quellcode von Programmen

Es gelten die Maßnahme 9.4.5 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

10 Kryptographie

10.1 Kryptographische Maßnahmen

Es gilt das Ziel von ISO/IEC 27002, 10.1.

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Es gelten die Maßnahme 10.1.1 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 kryptographische Maßnahmen für die Nutzung von Cloud-Diensten implementieren, sofern die Risikoanalyse dies rechtfertigt. Die Maßnahmen sollten ausreichend durchgreifend sein, um die ermittelten Risiken zu verringern, ungeachtet, ob diese Maßnahmen vom Cloud-Dienstleistungskunden oder vom Cloud-Dienstleister umgesetzt werden.</p> <p>Wenn der Cloud-Dienstleister Kryptographie anbietet, sollte der Cloud-Dienstleistungskunde alle vom Cloud-Dienstleister gelieferten Informationen überprüfen, ob die kryptographischen Kapazitäten</p> <ul style="list-style-type: none"> — die Anforderungen aus den Richtlinien des Cloud-Dienstleistungskunden erfüllen, — mit allen anderen kryptographischen Schutzmaßnahmen, die beim Cloud-Dienstleistungskunden eingesetzt wird, kompatibel sind, — für die Data-at-Rest und die Daten, die zum, vom oder innerhalb des Cloud-Dienstes übertragen werden, anwendbar sind. 	<p>Der Cloud-Dienstleister sollte dem Cloud-Dienstleistungskunden Informationen zu den Umständen zur Verfügung stellen, unter denen er kryptographische Mittel anwendet, um die von ihm verarbeiteten Informationen zu schützen. Der Cloud-Dienstleister sollte dem Cloud-Dienstleistungskunden außerdem Informationen zu den von ihm bereitgestellten Kapazitäten zur Verfügung stellen, die dem Cloud-Dienstleistungskunden bei der Anwendung seiner eigenen kryptographischen Schutzmaßnahmen helfen können.</p>

Sonstige Informationen für Cloud-Dienste

Einige Rechtssysteme könnten die Anwendung von kryptographischen Verfahren zum Schutz bestimmter Arten von Informationen verlangen, wie z. B. Gesundheitsdaten, Einwohnermeldenummern, Passnummern und Führerscheinnummern.

10.1.2 Schlüsselverwaltung

Es gelten die Maßnahme 10.1.2 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 die kryptographischen Schlüssel für jeden Cloud-Dienst identifizieren und Verfahren für die Schlüsselverwaltung umsetzen.</p> <p>Bietet der Cloud-Dienst eine Funktion für die Schlüsselverwaltung zum Gebrauch des Cloud-Dienstleistungskunden an, sollte der Cloud-Dienstleistungskunde die folgenden Informationen zu den Verfahren, die zur Verwaltung der Schlüssel im Bezug auf den Cloud-Dienst verwendet werden, anfordern:</p> <ul style="list-style-type: none">— Art der Schlüssel;— Spezifikationen des Schlüsselverwaltungssystems, einschließlich Verfahren für jede Phase des Lebenszyklus des Schlüssels, d. h. Erstellen, Ändern oder Aktualisieren, Speichern, Einziehen, Wiederherstellen, Sichern und Löschen;— empfohlene Verfahren für die Schlüsselverwaltung zum Gebrauch des Cloud-Dienstleistungskunden. <p>Der Cloud-Dienstleistungskunde sollte dem Cloud-Dienstleister nicht gestatten, die Kodierungsschlüssel für kryptographische Vorgänge zu speichern und zu verwalten, sofern der Cloud-Dienstleistungskunde seine eigene Schlüsselverwaltung oder einen anderen Dienst zur Schlüsselverwaltung nutzt.</p>	<p>(keine weitere Anleitung zur Umsetzung)</p>

11 Physische und umgebungsbezogene Sicherheit

11.1 Sicherheitsbereiche

Es gilt das Ziel von ISO/IEC 27002, 11.1.

11.1.1 Physische Sicherheitsperimeter

Es gelten die Maßnahme 11.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.1.2 Physische Zutrittssteuerung

Es gelten die Maßnahme 11.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.1.3 Sichern von Büros, Räumen und Einrichtungen

Es gelten die Maßnahme 11.1.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Es gelten die Maßnahme 11.1.4 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.1.5 Arbeiten in Sicherheitsbereichen

Es gelten die Maßnahme 11.1.5 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.1.6 Anlieferungs- und Ladebereiche

Es gelten die Maßnahme 11.1.6 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2 Geräte und Betriebsmittel

Es gilt das Ziel von ISO/IEC 27002, 11.2.

11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln

Es gelten die Maßnahme 11.2.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.2 Versorgungseinrichtungen

Es gelten die Maßnahme 11.2.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.3 Sicherheit der Verkabelung

Es gelten die Maßnahme 11.2.3 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.4 Instandhaltung von Geräten und Betriebsmitteln

Es gelten die Maßnahme 11.2.4 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.5 Entfernen von Werten

Es gelten die Maßnahme 11.2.5 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten

Es gelten die Maßnahme 11.2.6 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Es gelten die Maßnahme 11.2.7 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 sich die Bestätigung einholen, dass der Cloud-Dienstleister über Richtlinien und Verfahren für die sichere Entsorgung und Wiederverwendung von Ressourcen verfügt.	Der Cloud-Dienstleister sollte sicherstellen, dass Vorkehrungen für die sichere und zeitnahe Entsorgung und Wiederverwendung der Ressourcen (z. B. Geräte und Betriebsmittel, Datenspeicherung, Dateien und Speicher) getroffen werden.

Sonstige Informationen für Cloud-Dienste

Zusätzliche Informationen über die sichere Entsorgung sind in ISO/IEC 27040 zu finden.

11.2.8 Unbeaufsichtigte Benutzergeräte

Es gelten die Maßnahme 11.2.8 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Es gelten die Maßnahme 11.2.9 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

12 Betriebssicherheit

12.1 Betriebsabläufe und -verantwortlichkeiten

Es gilt das Ziel von ISO/IEC 27002, 12.1.

12.1.1 Dokumentierte Betriebsabläufe

Es gelten die Maßnahme 12.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

12.1.2 Änderungssteuerung

Es gelten die Maßnahme 12.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.