DIN EN ISO/IEC 27017

DIN

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 beigefügt. 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 — Informationssicherheitsmanagement-systeme — Überblick und Terminologie*

E DIN EN ISO/IEC 27001:2017-12, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-managementsysteme — 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 —

– Entwurf –

2020-08

prEN ISO/IEC 27017:2020

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