

# E DIN EN ISO/IEC 27017:2020-09 (D/E)

Erscheinungsdatum: 2020-08-21

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

---

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 Zugangssteuerung.....	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

<b>11</b>	<b>Physische und umgebungsbezogene Sicherheit.....</b>	<b>23</b>
11.1	Sicherheitsbereiche.....	23
11.2	Geräte und Betriebsmittel.....	24
<b>12</b>	<b>Betriebssicherheit .....</b>	<b>25</b>
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
<b>13</b>	<b>Kommunikationssicherheit.....</b>	<b>31</b>
13.1	Netzwerksicherheitsmanagement.....	31
13.2	Informationsübertragung .....	32
<b>14</b>	<b>Anschaffung, Entwicklung und Instandhaltung von Systemen.....</b>	<b>32</b>
14.1	Sicherheitsanforderungen an Informationssysteme.....	32
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen .....	33
14.3	Testdaten .....	34
<b>15</b>	<b>Lieferantenbeziehungen.....</b>	<b>34</b>
15.1	Informationssicherheit in Lieferantenbeziehungen .....	34
15.2	Steuerung der Dienstleistungserbringung von Lieferanten .....	36
<b>16</b>	<b>Handhabung von Informationssicherheitsvorfällen .....</b>	<b>36</b>
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....	36
<b>17</b>	<b>Informationssicherheitsaspekte beim Business Continuity Management.....</b>	<b>39</b>
17.1	Aufrechterhalten der Informationssicherheit.....	39
17.2	Redundanzen.....	39
<b>18</b>	<b>Compliance.....</b>	<b>39</b>
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen .....	39
18.2	Überprüfungen der Informationssicherheit .....	41
<b>Anhang A Erweiterungssatz von Maßnahmen für Cloud-Dienste .....</b>		<b>43</b>
<b>Anhang B Verweisungen zum Informationssicherheitsrisiko im Zusammenhang mit Cloud Computing .....</b>		<b>49</b>
<b>Literaturhinweise.....</b>		<b>51</b>