

# 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>
<b>11.1</b>	<b>Sicherheitsbereiche.....</b>	<b>23</b>
<b>11.2</b>	<b>Geräte und Betriebsmittel.....</b>	<b>24</b>
<b>12</b>	<b>Betriebssicherheit .....</b>	<b>25</b>
<b>12.1</b>	<b>Betriebsabläufe und -verantwortlichkeiten.....</b>	<b>25</b>
<b>12.2</b>	<b>Schutz vor Schadsoftware.....</b>	<b>27</b>
<b>12.3</b>	<b>Datensicherung.....</b>	<b>27</b>
<b>12.4</b>	<b>Protokollierung und Überwachung.....</b>	<b>28</b>
<b>12.5</b>	<b>Steuerung von Software im Betrieb .....</b>	<b>30</b>
<b>12.6</b>	<b>Handhabung technischer Schwachstellen.....</b>	<b>30</b>
<b>12.7</b>	<b>Audit von Informationssystemen.....</b>	<b>31</b>
<b>13</b>	<b>Kommunikationssicherheit.....</b>	<b>31</b>
<b>13.1</b>	<b>Netzwerksicherheitsmanagement.....</b>	<b>31</b>
<b>13.2</b>	<b>Informationsübertragung .....</b>	<b>32</b>
<b>14</b>	<b>Anschaffung, Entwicklung und Instandhaltung von Systemen.....</b>	<b>32</b>
<b>14.1</b>	<b>Sicherheitsanforderungen an Informationssysteme.....</b>	<b>32</b>
<b>14.2</b>	<b>Sicherheit in Entwicklungs- und Unterstützungsprozessen .....</b>	<b>33</b>
<b>14.3</b>	<b>Testdaten .....</b>	<b>34</b>
<b>15</b>	<b>Lieferantenbeziehungen.....</b>	<b>34</b>
<b>15.1</b>	<b>Informationssicherheit in Lieferantenbeziehungen .....</b>	<b>34</b>
<b>15.2</b>	<b>Steuerung der Dienstleistungserbringung von Lieferanten .....</b>	<b>36</b>
<b>16</b>	<b>Handhabung von Informationssicherheitsvorfällen .....</b>	<b>36</b>
<b>16.1</b>	<b>Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....</b>	<b>36</b>
<b>17</b>	<b>Informationssicherheitsaspekte beim Business Continuity Management.....</b>	<b>39</b>
<b>17.1</b>	<b>Aufrechterhalten der Informationssicherheit.....</b>	<b>39</b>
<b>17.2</b>	<b>Redundanzen.....</b>	<b>39</b>
<b>18</b>	<b>Compliance.....</b>	<b>39</b>
<b>18.1</b>	<b>Einhaltung gesetzlicher und vertraglicher Anforderungen .....</b>	<b>39</b>
<b>18.2</b>	<b>Überprüfungen der Informationssicherheit .....</b>	<b>41</b>
	<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>