

DIN EN ISO/IEC 27001:2017 Anhang A (Normativ)

A5 Informationssicherheitsrichtlinien	A.6 Organisation der Informationssicherheit	A.7 Personalsicherheit	A.8 Verwaltung der Werte	A.9 Zugangssteuerung	A.10 Kryptographie	A.11 Physische und umgebungsbezogene Sicherheit	
A.5.1 Vorgaben der Leitung für Informationssicherheit	A.6.1 Interne Organisation A.6.2 Mobilgeräte & Telearbeit	A.7.1 Vor der Beschäftigung A.7.2 Während der Beschäftigung A.7.3 Beendigung und Änderung der Beschäftigung	A.8.1 Verantwortlichkeit für Werte A.8.2 Informationsklassifizierung A.8.3 Handhabung von Datenträgern	A.9.1 Geschäftsanforderungen an die Zugangssteuerung A.9.2 Benutzerzugangsverwaltung A.9.3 Benutzerverantwortlichkeiten A.9.3 Benutzerverantwortlichkeiten	A.10.1 Kryptographische Maßnahmen	A.11.1 Sicherheitsbereiche A.11.2 Geräte und Betriebsmittel	
A.12 Betriebssicherheit (1/2)	A.12 Betriebssicherheit (2/2)	A.13 Kommunikationssicherheit	A.14 Anschaffung, Entwicklung & Instandhalten von Systemen	A.15 Lieferantenbeziehungen	A.16 Handhabung von Informationssicherheitsvorfällen	A.17 IS-Aspekte beim Business Continuity Management	A.18 Compliance
A.12.1 Betriebsabläufe und - A.12.2 Schutz vor Schadsoftware A.12.3 Datensicherung	A.12.4 Protokollierung & Überwachung A.12.5 Steuerung von Software im Betrieb A.12.6 Handhabung technischer Schwachstellen A.12.7 Audit von Info-Systemen	A.13.1 Netzwerksicherheitsmanagement A.13.2 Informationsübertragung	A.14.1 Sicherheitsanforderungen an Info-Systeme A.14.2 Sicherheit in Entwicklungs- & Unterstützungsprozessen A.14.3 Testdaten	A.15.1 Informationssicherheit in Lieferantenbeziehungen A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten	A.16.1 Handhabung von Informationssicherheitsvorfällen & Verbesserungen	A.17.1 Aufrechterhalten der Informationssicherheit A.17.2 Redundanzen	A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen A.18.2 Überprüfungen der Informationssicherheit