

DIN EN ISO/IEC 27001:2017-06 (D)

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

Inhalt	Seite
Europäisches Vorwort.....	3
Vorwort	4
0 Einleitung.....	5
1 Anwendungsbereich.....	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Kontext der Organisation	6
4.1 Verstehen der Organisation und ihres Kontextes	6
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien.....	6
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems.....	7
4.4 Informationssicherheitsmanagementsystem	7
5 Führung	7
5.1 Führung und Verpflichtung.....	7
5.2 Politik.....	8
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.....	8
6 Planung.....	8
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	8
6.2 Informationssicherheitsziele und Planung zu deren Erreichung.....	10
7 Unterstützung.....	11
7.1 Ressourcen	11
7.2 Kompetenz.....	11
7.3 Bewusstsein	11
7.4 Kommunikation	12
7.5 Dokumentierte Information	12
8 Betrieb	13
8.1 Betriebliche Planung und Steuerung.....	13
8.2 Informationssicherheitsrisikobeurteilung.....	13
8.3 Informationssicherheitsrisikobehandlung.....	14
9 Bewertung der Leistung.....	14
9.1 Überwachung, Messung, Analyse und Bewertung	14
9.2 Internes Audit.....	14
9.3 Managementbewertung	15
10 Verbesserung.....	16
10.1 Nichtkonformität und Korrekturmaßnahmen	16
10.2 Fortlaufende Verbesserung	16
Anhang A (normativ) Referenzmaßnahmenziele und -maßnahmen.....	17
Literaturhinweise	31