

E DIN EN ISO/IEC 27001:2023-04 (D/E)

Erscheinungsdatum: 2023-03-17

Informationssicherheit, Cybersicherheit und Datenschutz -
Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022);
Deutsche und Englische Fassung prEN ISO/IEC 27001:2023

Information security, cybersecurity and privacy protection - Information security
management systems - Requirements (ISO/IEC 27001:2022); German and English
version prEN ISO/IEC 27001:2023

Inhalt	Seite
Europäisches Vorwort.....	7
Vorwort.....	8
Einleitung.....	9
1 Anwendungsbereich.....	10
2 Normative Verweisungen.....	10
3 Begriffe.....	10
4 Kontext der Organisation.....	10
4.1 Verstehen der Organisation und ihres Kontextes.....	10
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien.....	10
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems.....	11
4.4 Informationssicherheitsmanagementsystem.....	11
5 Führung.....	11
5.1 Führung und Verpflichtung.....	11
5.2 Politik.....	12
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.....	12
6 Planung.....	12
6.1 Maßnahmen zum Umgang mit Risiken und Chancen.....	12
6.1.1 Allgemeines.....	12
6.1.2 Informationssicherheitsrisikobeurteilung.....	13
6.1.3 Informationssicherheitsrisikobehandlung.....	14
6.2 Informationssicherheitsziele und Planung zu deren Erreichung.....	14
6.3 Planung von Änderungen.....	15
7 Unterstützung.....	15
7.1 Ressourcen.....	15
7.2 Kompetenz.....	15
7.3 Bewusstsein.....	16
7.4 Kommunikation.....	16
7.5 Dokumentierte Information.....	16
7.5.1 Allgemeines.....	16
7.5.2 Erstellen und Aktualisieren.....	16
7.5.3 Lenkung dokumentierter Information.....	17
8 Betrieb.....	17
8.1 Betriebliche Planung und Steuerung.....	17
8.2 Informationssicherheitsrisikobeurteilung.....	17
8.3 Informationssicherheitsrisikobehandlung.....	18
9 Bewertung der Leistung.....	18

9.1	Überwachung, Messung, Analyse und Bewertung	18
9.2	Internes Audit.....	18
9.2.1	Allgemeines.....	18
9.2.2	Internes Auditprogramm.....	19
9.3	Managementbewertung	19
9.3.1	Allgemeines.....	19
9.3.2	Eingaben für die Managementbewertung.....	19
9.3.3	Ergebnisse der Managementbewertung.....	20
10	Verbesserung.....	20
10.1	Fortlaufende Verbesserung	20
10.2	Nichtkonformität und Korrekturmaßnahmen	20
Anhang A (normativ) Verweisung auf Informationssicherheitsmaßnahmen		21
Literaturhinweise		30

Tabellen

Tabelle A.1 — Informationssicherheitsmaßnahmen.....	21
---	----