

E DIN ISO/IEC 27001:2014-02 (D)

Erscheinungsdatum: 2014-01-10

Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits- Managementsysteme - Anforderungen (ISO/IEC DIS 27001:2013)

Inhalt	Seite
Nationales Vorwort	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
0 Einleitung	5
0.1 Allgemeines	5
0.2 Kompatibilität mit anderen Normen für Managementsysteme	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Kontext der Organisation	6
4.1 Verständnis der Organisation und ihres Kontexts	6
4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien	6
4.3 Festlegung des Geltungsbereichs des Informationssicherheitsmanagementsystems	7
4.4 Informationssicherheitsmanagementsystem	7
5 Führung	7
5.1 Führung und Engagement	7
5.2 Leitlinie	8
5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse	8
6 Planung	8
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	8
6.2 Informationssicherheitsziele und Pläne für 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 Informationen	12
8 Einsatz	13
8.1 Einsatzplanung und -kontrolle	13
8.2 Informationssicherheitsrisikoeinschätzung	13
8.3 Informationssicherheitsrisikobehandlung	13
9 Leistungsauswertung	14
9.1 Überwachung, Messung, Analyse und Auswertung	14
9.2 Internes Audit	14
9.3 Prüfung durch die Leitung	15
10 Verbesserung	15
10.1 Fehler und Korrekturmaßnahmen	15
10.2 Laufende Verbesserung	16
Anhang A (normativ) Referenz-Maßnahmenziele und Maßnahmen	17
Literaturhinweise	32