## **DIN EN ISO/IEC 27001:2024-01 (D)**

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

Inhalt		Seite	
Europ	äisches Vorwort	7	
Vorwo	ort	8	
Einlei	tung	9	
1	Anwendungsbereich		
2	Normative Verweisungen	10	
3	Begriffe		
4	Kontext der Organisation		
4 4.1	Verstehen der Organisation und ihres Kontextes		
4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien		
4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems		
4.4	Informationssicherheitsmanagementsystem		
5	Führung	11	
5.1	Führung und Verpflichtung	11	
5.2	Politik		
5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	12	
6	Planung	12	
6.1	Maßnahmen zum Umgang mit Risiken und Chancen		
6.1.1	Allgemeines		
6.1.2	Informationssicherheitsrisikobeurteilung		
6.1.3	Informationssicherheitsrisikobehandlung		
6.2	Informationssicherheitsziele und Planung zu deren Erreichung		
6.3	Planung von Änderungen	15	
7	Unterstützung		
7.1	Ressourcen		
7.2	Kompetenz		
7.3	Bewusstsein		
7.4	Kommunikation		
7.5 7.5.1	Dokumentierte Information		
7.5.1 7.5.2	Erstellen und Aktualisieren		
7.5.3	Steuerung dokumentierter Information		
8 8.1	BetriebBetriebliche Planung und Steuerung		
8.1	Informationssicherheitsrisikobeurteilung		
8.3	Informationssicherheitsrisikobehandlung		
	G		
9	Bewertung der Leistung	18	
9.1	Überwachung, Messung, Analyse und Bewertung		
9.2 9.2.1	Internes AuditAllgemeines		
9.2.1	Internes Auditprogramm		
9.2.2	Managementbewertung		

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		20
10.2	Nichtkonformität und Korrekturmaßnahmen	20
Anhar	ng A (normativ) Verweisung auf Informationssicherheitsmaßnahmen	21
Litera	turhinweise	30
Tabell	len	
Tabel	le A.1 — Informationssicherheitsmaßnahmen	21