

Inhalt

Zur Nutzung der Broschüre.....	3
1 Bedeutung der Informationssicherheit.....	7
2 Ziel und Zweck der ISO/IEC 27001:2022.....	13
3 Die ISO/IEC 27001, Harmonized Structure und IMS-Integration	17
3.1 Struktur der ISO/IEC 27001 (inkl. HS).....	17
3.2 Revision ISO/IEC 27001:2022 – Was gibt es Neues?	19
4 Beziehung zu weiteren Normen und Regelwerken.....	25
4.1 Weitere Normen zum Informationssicherheitsmanagement	25
4.2 Zusammenspiel mit anderen ISO-Managementsystemnormen ..	28
4.3 IT-Grundschutz des BSI.....	29
5 Regulative Forderungen in der Informationssicherheit.....	33
6 Integration der Forderungen des ISMS in ein IMS	37
6.1 Einführung	37
6.2 Kontext der Organisation.....	39
6.2.1 Verstehen der Organisation und ihres Kontextes	39
6.2.2 Erfordernisse und Erwartungen interessierter Parteien	39
6.2.3 Festlegen des Anwendungsbereichs des ISMS	40
6.2.4 Informationssicherheitsmanagementsystem	40
6.3 Führung	41
6.3.1 Führung und Verpflichtung	41
6.3.2 (Informationssicherheits-)Politik	41
6.3.3 Rollen, Verantwortlichkeiten und Befugnisse	42
6.4 Planung	43
6.4.1 Umgang mit Risiken und Chancen.....	43
6.4.2 Informationssicherheitsziele und Planung zur Erreichung ..	46
6.4.3 Planung von Änderungen	47
6.5 Unterstützung	48
6.5.1 Ressourcen	48
6.5.2 Kompetenz	48
6.5.3 Bewusstsein	49
6.5.4 Kommunikation.....	49
6.5.5 Dokumentierte Information.....	50
6.6 Betrieb	52
6.6.1 Betriebliche Planung und Steuerung.....	52
6.6.2 „Betrieb“ potenzielle operative Prozesse im ISMS.....	53
6.6.3 Informationssicherheitsrisikobeurteilung.....	62
6.6.4 Informationssicherheitsrisikobehandlung	63
6.7 Bewertung der Leistung	63
6.7.1 Überwachung, Messung, Analyse und Bewertung.....	63
6.7.2 Internes Audit.....	64
6.7.3 Managementbewertung.....	65
6.8 Verbesserung	67
6.8.1 Fortlaufende Verbesserung	67
6.8.2 Nichtkonformität und Korrekturmaßnahmen	68
Quellen.....	71