Thematische Zuordnung der Maßnahmen aus DIN EN ISO/IEC 27001:2024

Oberthemen	Kap.	Organisatorische Maßnahmen
Interne Organisation	A.5.1	Informationssicherheitspolitik und -richtlinien
	A.5.2	Informationssicherheitsrollen und Verantwortlichkeiten
	A.5.3	Aufgabentrennung
	A.5.4	Verantwortlichkeiten der Leitung
	A.5.5	Kontakte zu Behörden
	A.5.6	Kontakt zu speziellen Interessengruppen
	A.5.7	**Informationen über die Bedrohungslage**
	A.5.8	Informationssicherheit im Projektmanagement
Werte-verwaltung	A.5.9	Inventar der Informationen und anderen damit verbundenen Werte
	A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
	A.5.11	Rückgabe von Werten
	A.5.12	Klassifizierung von Information
	A.5.13	Kennzeichnung von Information
	A.5.14	Informationsübermittlung
Rechte-Verwaltung	A.5.15	Zugangssteuerung
	A.5.16	Identitätsmanagement
	A.5.17	Authentisierungsinformationen
	A.5.18	Zugangsrechte
Lieferanten-beziehungen	A.5.19	Informationssicherheit in Lieferantenbeziehungen
	A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen
	A.5.21	Umgang mit der Informationssicherheit in der Lieferkette der IK-Technolgie
	A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
	A.5.23	**Informationssicherheit für die Nutzung von Cloud-Diensten**
Informations-sicherheits-vorfälle	A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
	A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse
	A.5.26	Reaktion auf Informationssicherheitsvorfälle
	A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen
	A.5.28	Sammeln von Beweismaterial
	A.5.29	Informationssicherheit bei Störungen
	A.5.30	**IKT-Bereitschaft für Business-Continuity**
Compliance	A.5.31	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen
	A.5.32	Geistige Eigentumsrechte
	A.5.33	Schutz von Aufzeichnungen
	A.5.34	Datenschutz und Schutz von personenbezogenen Daten (PbD)
	A.5.35	Unabhängige Überprüfung der Informationssicherheit
	A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
Dokumentation	A.5.37	Dokumentierte Betriebsabläufe

Oberthemen	Kap.	Personenbezogene Maßnahmen
Vor der Beschäftigung	A.6.1	Sicherheitsüberprüfung
	A.6.2	Beschäftigungs- und Vertragsbedingungen
Während der Beschäftigung	A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung
	A.6.4	Maßregelungsprozess
Nach der Beschäftigung	A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
	A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen
Mobiles Arbeiten	A.6.7	Remote-Arbeit
Meldeprozess	A.6.8	Meldung von Informationssicherheitsereignissen

Oberthemen	Kap.	Physische Maßnahmen
Physische Sicherheit	A.7.1	Physische Sicherheitsperimeter
	A.7.2	Physischer Zutritt
	A.7.3	Sichern von Büros, Räumen und Einrichtungen
	A.7.4	**Physische Sicherheitsüberwachung**
	A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen
Arbeitsplätze	A.7.6	Arbeiten in Sicherheitsbereichen
	A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren
Umgang mit Werten	A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln
	A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten
Betriebsmittel	A.7.10	Speichermedien
	A.7.11	Versorgungseinrichtungen
	A.7.12	Sicherheit der Verkabelung
Wartung und Entsorgung	A.7.13	Instandhaltung von Geräten und Betriebsmitteln
	A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Oberthemen	Kap.	Technologische Maßnahmen
Zugangs-sicherheit	A.8.1	Endpunktgeräte des Benutzers
	A.8.2	Privilegierte Zugangsrechte
	A.8.3	Informationszugangsbeschränkung
	A.8.4	Zugriff auf den Quellcode
	A.8.5	Sichere Authentisierung
Betriebs-sicherheit	A.8.6	Kapazitätssteuerung
	A.8.7	Schutz gegen Schadsoftware
	A.8.8	Handhabung von technischen Schwachstellen
	A.8.9	**Konfigurationsmanagement**
Daten-sicherheit	A.8.10	**Löschung von Informationen**
	A.8.11	**Datenmaskierung**
	A.8.12	**Verhinderung von Datenlecks**
	A.8.13	Sicherung von Informationen
Administration	A.8.14	Redundanz von informationsverarbeitenden Einrichtungen
	A.8.15	Protokollierung
	A.8.16	**Überwachung von Aktivitäten**
	A.8.17	Uhrensynchronisation
	A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten
	A.8.19	Installation von Software auf Systemen im Betrieb
Netzsicherheit	A.8.20	Netzwerksicherheit
	A.8.21	Sicherheit von Netzwerkdiensten
	A.8.22	Trennung von Netzwerken
	A.8.23	**Webfilterung**
	A.8.24	Verwendung von Kryptographie
Entwicklungs-sicherheit	A.8.25	Lebenszyklus einer sicheren Entwicklung
	A.8.26	Anforderungen an die Anwendungssicherheit
	A.8.27	Sichere Systemarchitektur und Entwicklungsgrundsätze
	A.8.28	**Sichere Codierung**
	A.8.29	Sicherheitsüberprüfung in Entwicklung und Abnahme
	A.8.30	Ausgegliederte Entwicklung
	A.8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen
	A.8.32	Änderungssteuerung
	A.8.33	Testdaten
Technische Überprüfungen	A.8.34	Schutz der Informationssysteme während Tests im Rahmen von Audits

 Buch-Quelle: ISO/IEC 27001 ISO/IEC 27002 und IT-Grundschutz, Schnelleinstieg Informationssicherheit, ISBN-13: 978-3756815494, Erstausgabe: 10.2022 mit DIN Buch-Lizenz

Übersicht der Normkapitel aus DIN EN ISO/IEC 27001:2024

0 Einleitung	1 Anwendungsbereich	2 Normative Verweisungen	3 Begriffe			
PLAN			DO		CHECK	ACT
4 Kontext der Organisation	5 Führung	6 Planung	7 Unterstützung	8 Betrieb	9 Bewertung der Leistung	10 Verbesserung
4.1 Verstehen der Organisation und ihres Kontextes	5.1 Führung und Verpflichtung	6.1 Maßnahmen zum Umgang mit Risiken und Chancen	7.1 Ressourcen	8.1 Betriebliche Planung und Steuerung	9.1 Überwachung, Messung, Analyse und Bewertung	10.1 Fortlaufende Verbesserung
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	5.2 Politik	6.2 Informations-sicherheitsziele und Planung zu deren Erreichung	7.2 Kompetenz	8.2 Informations-sicherheitsrisiko-beurteilung	9.2 Internes Audit	10.2 Nichtkonformitäten und Korrekturmaßnahmen
4.3 Festlegen des Anwendungsbereichs des ISMS	5.3 Rollen, Verantwort-lichkeiten und Befugnisse der Organisation	6.3 Planung von Änderungen	7.3 Bewusstsein	8.3 Informations-sicherheitsrisiko-behandlung	9.3 Managementbewertung	
4.4 Informationssicherheits-managementsystem			7.4 Kommunikation			
			7.5 Dokumentierte Information			