ORIENTIERUNGSHILFE FÜR DIE GESCHÄFTSLEITUNG

ISO 27001 Werkzeugkasten: die zehn Themenfelder

Was jedes Themenfeld erreichen soll und mit welchen Lösungsklassen es typischerweise umgesetzt wird, herstellerneutral.

Themenfeld (Abgleich mit Annex A)	Ziel in einem Satz	Typische Lösungsklassen (Auswahl)
1 Risikomanagement & Leitlinie	Risiken kennen, bewerten und priorisieren	Asset-Inventar, Schwachstellenscanner, GRC-/ISMS-Tool, Risikoregister
2 Vorfallsmanagement	Angriffe schnell erkennen, eindämmen und beheben	EDR/XDR, SIEM oder Managed Detection (MDR), Incident-Response-Playbooks und -Retainer
3 Betriebskontinuität & Notfall	Nach Störungen schnell wieder lieferfähig sein	Backup mit Offline-Kopie und Restore-Tests, Notfallhandbuch, Krisenstabsübung
4 Lieferanten & Dienstleister	Risiken aus Dienstleistern und Zulieferern beherrschen	Lieferantenbewertung, Sicherheitsanhänge in Verträgen, kontrollierte Fernwartungszugänge (VPN/ZTNA)
5 Beschaffung & Entwicklung	Sicherheit einkaufen statt teuer nachrüsten	Patch- und Änderungsmanagement, Härtungsvorgaben, Penetrationstests
6 Audits & Wirksamkeit	Belegen, dass die Maßnahmen wirken	Interne Audits, Kennzahlen-Reporting, Phishing-Tests, Management-Review
7 Awareness & Schulung	Mitarbeitende zur ersten Verteidigungslinie machen	Awareness-Plattform, Phishing-Simulation, Verwaltung der Schulungsnachweise
8 Kryptografie	Daten bei Speicherung und Übertragung schützen	Festplatten- und E-Mail-Verschlüsselung, TLS-Konfiguration, Schlüsselverwaltung
9 Personal & Zugriffe	Nur berechtigte Personen an die richtigen Daten lassen	Berechtigungskonzept, IAM, Schutz privilegierter Konten (PAM), sauberes On- und Offboarding
10 Zugangsschutz & MFA	Konten und Kommunikationswege absichern	MFA/SSO, gehärtete Remote-Zugänge, sichere Messenger- und Konferenzlösungen

Lösungsklassen statt Produkte: Die Auswahl folgt Risiko, Größe und Bestand und wird in der SoA begründet. Vieles ist in vorhandenen Lizenzen (z. B. Microsoft 365 Business Premium) bereits enthalten und muss nur aktiviert werden. Stand: Juli 2026.

David Zion · vCISO & strategischer Security- und Compliance-Berater · davidzion.de