Technische und organisatorische Maßnahmen

Kontrollkatalog für ein risikogerechtes Schutzniveau und die regelmäßige Wirksamkeitsprüfung.

Version 1.0 | Stand 18.08.2026 | Prüfgrundlage

Versorgia - Technische und organisatorische Maßnahmen
Version: 1.0
Stand: 18.08.2026
Status: Prüfgrundlage
Zielgruppen: Informationssicherheit, Datenschutz, Revision

Prüfziel
Kontrollkatalog für ein risikogerechtes Schutzniveau und die regelmäßige Wirksamkeitsprüfung.

1. Vertraulichkeit
- Mandantentrennung, Rollen und Rechte, starke Anmeldung, Sitzungsgrenzen und administrativen Zugriff prüfen.
- Verschlüsselung bei Übertragung und Speicherung, Schlüsselverwaltung und sichere Geheimnisablage nachweisen.

2. Integrität und Nachvollziehbarkeit
- Eingabevalidierung, fachliche Freigaben, unveränderbare Snapshots, verkettete Ereignisprotokolle und dokumentierte Änderungen prüfen.
- Manipulationsschutz für Rechnungs-, Zahlungs-, Markt- und Nachweisdokumente belegen.

3. Verfügbarkeit und Belastbarkeit
- Kapazitätsüberwachung, Sicherung, Wiederherstellung, Notbetrieb und Wiederanlaufziele dokumentieren und testen.
- Abhängigkeiten von Rechenzentrum, DNS, Zertifikaten, Transportwegen und externen Diensten erfassen.

4. Regelmäßige Überprüfung

- Kontrollverantwortliche, Prüfintervall, Stichprobe, Ergebnis, Abweichung und Maßnahmenverfolgung festlegen.
- Schwachstellenprüfung, Wiederherstellungstest und Berechtigungsrezertifizierung als wiederkehrende Nachweise führen.

5. Quellen und Prüfmaßstab

- DSGVO, insbesondere Art. 28, 30, 32 und 33: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de
- § 30 BSIG: Risikomanagementmaßnahmen: https://www.gesetze-im-internet.de/bsig_2025/__30.html

Einordnung

Dieses Dokument ist eine strukturierte Prüf- und Abstimmungsgrundlage. Es ist kein Zertifikat, kein Prüfbericht einer unabhängigen Stelle und keine Rechtsberatung. Offene Betreiber-, Hosting-, Vertrags- und Abnahmeangaben müssen vor Produktivfreigabe mit Nachweisen ergänzt und von den zuständigen Stellen freigegeben werden.

Öffentliche Prüfgrundlage von Versorgia. Kein Zertifikat, kein unabhängiges Testat und keine Rechtsberatung.