ISO 27001 Cheat-Sheet — dokumentiert ist nicht wirksam

16 Kontrollbereiche nach ISO 27001:2022, vier Reifegrade: Policy · Procedure · Implementation · Evidence

Policy Ist es vorgegeben? **Procedure** Ist beschrieben, wie? **Implementation** Läuft es wirklich? **Evidence** Ist es nachweisbar?

	DOKUMENTIERT		WIRKSAM	
KONTROLLBEREICH	POLICY	PROCEDURE	IMPLEMENTATION	EVIDENCE
01 **Sicherheitsrichtlinien & Governance** ISO 27002: 5.1, 5.36, 5.37	ISMS-Leitlinie, von der Leitung freigegeben	Review-Zyklus, Freigabe- und Verteilweg	Richtlinien bekannt und jährlich überprüft	Freigabe-Datum, Versionshistorie, Review-Protokoll
02 **Rollen & Verantwortlichkeiten** ISO 27002: 5.2 – 5.4	Rollen, Zuständigkeiten, Funktionstrennung definiert	Rollenbeschreibungen, RACI, Eskalationswege	Rollen besetzt, Funktionstrennung wirksam	Org-Chart, Rollenmatrix, CISO-Bestellung
03 **Asset- & Informationsmanagement** ISO 27002: 5.9 – 5.13	Klassifizierungs- und Asset-Vorgaben	Inventar-Pflege, Labelling-Schema, Rückgabe	Inventar aktuell, Daten klassifiziert	Asset-Register, Klassifizierungs-Stichprobe
04 **Zugriffskontrolle & Identitäten** ISO 27002: 5.15 – 5.18, 8.2, 8.3, 8.5	Berechtigungskonzept nach Least Privilege	Antrag/Genehmigung, Rezertifizierung, MFA-Vorgabe	Rechte bedarfsgerecht, MFA aktiv, Rezert. läuft	Berechtigungs-Export, Rezertifizierungs-Protokoll
05 **Lieferanten & Lieferkette** ISO 27002: 5.19 – 5.23	Anforderungen an Lieferanten und Cloud-Nutzung	Onboarding, Vertragsklauseln, Audit-Recht	Lieferanten bewertet, Verträge geschärft	Lieferantenregister, Verträge, Bewertungen
06 **Incident-Management** ISO 27002: 5.5, 5.6, 5.24 – 5.28, 6.8	Melde- und Reaktionspflichten festgelegt	Runbooks, Eskalation, Beweissicherung, Behördenkontakt	Vorfälle erkannt, gemeldet, ausgewertet	Ticket-Historie, Post-Incident-Reports
07 **Business Continuity & Resilienz** ISO 27002: 5.29, 5.30, 8.13, 8.14	Continuity- und Backup-Vorgaben (RTO/RPO)	BCP, Backup-Plan, Wiederanlauf-Tests	Backups laufen, Restore getestet	Restore-Test-Protokoll, Übungsbericht
08 **Compliance & Recht** ISO 27002: 5.31 – 5.35	Rechts-, Datenschutz- und Aufbewahrungsvorgaben	Pflichtenregister, unabhängige Reviews	Anforderungen erfüllt, Reviews durchgeführt	Compliance-Register, Review-/Auditberichte
09 **Personal & Awareness** ISO 27002: 6.1 – 6.7	HR-Sicherheitsvorgaben, NDA, Remote-Work-Regeln	Screening, On-/Offboarding, Schulungsplan	Schulungen absolviert, Offboarding sauber	Schulungsnachweise, NDA-Akten, Teilnahmequote
10 **Physische Sicherheit** ISO 27002: 7.1 – 7.14	Zutritts- und Umgebungs-Sicherheitsvorgaben	Zutrittssteuerung, Clear-Desk, Entsorgung	Zonen gesichert, Zutritt protokolliert	Zutrittslogs, Begehungsprotokoll
11 **Bedrohungs- & Schwachstellenmanagement** ISO 27002: 5.7, 8.7, 8.8	Vorgaben zu Patch, Malware-Schutz, Threat Intel	Patch-Zyklus, Scan-Plan, Bewertung	Patches eingespielt, Scans laufen	Scan-Reports, Patch-Status, SLA-Einhaltung
12 **Betrieb, Konfiguration & Change** ISO 27002: 8.1, 8.6, 8.9, 8.19, 8.32	Härtungs-, Change- und Kapazitäts-Vorgaben	Baselines, Change-Prozess, Kapazitätsplanung	Systeme gehärtet, Changes kontrolliert	Konfig-Baselines, Change-Tickets, CAB-Protokoll
13 **Netzwerksicherheit** ISO 27002: 8.20 – 8.23	Segmentierungs- und Filter-Vorgaben	Firewall-Regelwerk, Segmentierung, Web-Filter	Segmente getrennt, Regeln aktuell	Firewall-Regel-Review, Netz-Diagramm
14 **Daten, Krypto & Lebenszyklus** ISO 27002: 5.14, 8.10 – 8.12, 8.24	Verschlüsselungs- und Datenschutz-Vorgaben	Schlüssel-Management, Löschkonzept, DLP-Regeln	Verschlüsselung aktiv, Löschung dokumentiert	Krypto-Inventar, Löschnachweise, DLP-Logs
15 **Sichere Entwicklung (SDLC)** ISO 27002: 5.8, 8.4, 8.25 – 8.31, 8.33, 8.34	Secure-SDLC- und Coding-Vorgaben	Security-Requirements, Code-Review, Test-Gates	Security-Tests in der Pipeline, Umgebungen getrennt	Test-Reports, Code-Review-Records, Freigaben
16 **Logging & Monitoring** ISO 27002: 8.15 – 8.18	Protokollierungs- und Monitoring-Vorgaben	Log-Quellen, Aufbewahrung, Alarmierung	Logs zentral, Alarme greifen, Zeit synchron	SIEM-Auswertung, Log-Aufbewahrungsnachweis