ISO 27001:2022 · STAGE 2

Stage 2 Evidence Checklist

Certification Audit nach ISO 27001:2022 — 60-Punkte-Check

VERSION
1.0

STAND
4. Juni 2026

LIZENZ
Creative Commons CC-BY-4.0

Ausfüllhinweise

Diese Checkliste strukturiert deine Stage-2-Vorbereitung (Certification Audit) nach ISO 27001:2022. Stage 2 prüft die operative Umsetzung deines ISMS durch Stichproben, Interviews und technische Verifikation. Jede Zeile repräsentiert ein Evidenz-Artefakt, das der Auditor üblicherweise einsieht.

Legende

1. Status: Ready = Evidenz liegt vollständig vor; Gap = Nachweis fehlt oder ist lückenhaft; N/A = für unseren Scope nicht anwendbar
2. Evidence Location: Pfad, Ticket-ID oder URL zum Nachweis
3. Kategorien entsprechen den vier Annex-A-Themenbereichen plus Audit-Logistik

A.5 — Organisatorische Controls

û	Control	Nachweis / Evidence	Status	Evidence Location
☐	A.5.1	Informationssicherheitsrichtlinien veröffentlicht, Kenntnisnahme dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.2	Rollen-Matrix mit Zuordnung der ISMS-Verantwortlichkeiten	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.3	Nachweis der Aufgabentrennung (SoD-Matrix, Rezertifizierungen)	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.4	Management-Commitment-Statement und Review-Zyklen	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.7	Threat-Intelligence-Quellen dokumentiert, Berichte archiviert	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.8	Projektmanagement-Leitlinie mit Security-Gates für Projekte	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.9	Asset-Inventory vollständig, mit Owner, Klassifizierung und Review-Datum	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.10	Acceptable-Use-Policy unterschrieben von allen Mitarbeitenden	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.12	Informationsklassifizierungs-Schema dokumentiert und angewandt	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.15	Access-Control-Matrix aktuell, Rezertifizierungs-Logs vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.16	Identity-Management-Prozess mit Onboarding- und Offboarding-Logs	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.17	MFA aktiviert, Ausnahmeliste dokumentiert und begründet	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.18	Zugangsrechte regelmäßig überprüft, Review-Protokolle vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.19	Lieferantenregister vollständig, Kritikalität bewertet	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.20	Security-Klauseln in allen Lieferantenverträgen dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.21	ICT-Supply-Chain-Risikobewertung vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.22	Lieferantenaudits durchgeführt und protokolliert	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.23	Cloud-Security-Richtlinie und genehmigte Cloud-Services-Liste	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.24	Incident-Response-Plan mit Eskalationskette und Kontakten	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.26	Incident-Log mit Detection, Response und Lessons Learned	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.29	Disruption-Planning: Ausfallkonzepte für kritische Prozesse	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.30	BCM / DR Test durchgeführt, Protokoll und Lessons Learned archiviert	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.31	Register der regulatorischen und vertraglichen Anforderungen	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.34	DSGVO-Prozesse: DSFA, Auftragsverarbeitung, Betroffenenrechte	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.35	Nachweis unabhängiger ISMS-Überprüfung (internes Audit)	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.37	Betriebsverfahren dokumentiert, versioniert, zugänglich	☐ Ready ☐ Gap ☐ N/A	

A.6 — Personenbezogene Controls

û	Control	Nachweis / Evidence	Status	Evidence Location
☐	A.6.1	Background-Checks für neue Mitarbeitende dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.2	Beschäftigungsverträge mit Security-Verpflichtungen	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.3	Awareness-Schulungen durchgeführt, Teilnahme zu 100 Prozent dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.4	Disziplinarprozess dokumentiert, Anwendung nachweisbar	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.5	Offboarding-Checklisten mit Rückgabe und Zugangsentzug	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.6	NDA-Register aktuell für alle relevanten Personen und Lieferanten	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.7	Remote-Work-Richtlinie, technische Absicherung nachweisbar	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.8	Meldekanäle für Security-Events eingerichtet und kommuniziert	☐ Ready ☐ Gap ☐ N/A	

A.7 — Physische Controls

û	Control	Nachweis / Evidence	Status	Evidence Location
☐	A.7.1	Perimeter-Schutz dokumentiert, Zutrittspunkte definiert	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.2	Zutrittskontrolle mit Logging, Besucherregister vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.3	Sicherung von Räumen mit kritischer Infrastruktur	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.4	Physische Überwachung (Kameras, Alarme) betriebsbereit	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.5	Schutz vor Brand, Wasser, Umwelt dokumentiert und getestet	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.7	Clear-Desk- und Clear-Screen-Policy umgesetzt	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.9	Schutzkonzept für Assets außerhalb der Geschäftsräume	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.10	Umgang mit Wechselmedien, Verschlüsselungsrichtlinie	☐ Ready ☐ Gap ☐ N/A	
☐	A.7.14	Sichere Entsorgungsnachweise für Hardware und Medien	☐ Ready ☐ Gap ☐ N/A	

A.8 — Technologische Controls

û	Control	Nachweis / Evidence	Status	Evidence Location
☐	A.8.1	Endpoint-Management: MDM, Verschlüsselung, Antivirus aktiv	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.2	Privilegierte Accounts mit dedizierten Admin-IDs und MFA	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.5	Sichere Authentifizierung (MFA, Passwort-Policy) überall aktiv	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.7	Malware-Schutz zentral gemanagt, Alert-Logs vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.8	Vulnerability-Scans über mindestens 6 Monate, Remediation-Tracking	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.9	Konfigurations-Baselines für Server und Endpoints	☐ Ready ☐ Gap ☐ N/A	

☐	A.8.10	Sichere Löschverfahren für sensible Daten dokumentiert	☐ Ready	☐ Gap	☐ N/A
☐	A.8.12	Data-Leakage-Prevention-Kontrollen aktiv und monitored	☐ Ready	☐ Gap	☐ N/A
☐	A.8.13	Backup-Konzept aktiv, Restore-Tests mit Protokoll	☐ Ready	☐ Gap	☐ N/A
☐	A.8.15	Logging zentral, mit Retention-Richtlinie und Zugriffsschutz	☐ Ready	☐ Gap	☐ N/A
☐	A.8.16	Monitoring und SIEM-Alerts mit dokumentierten Use Cases	☐ Ready	☐ Gap	☐ N/A
☐	A.8.20	Netzwerksegmentierung und Firewall-Policies dokumentiert	☐ Ready	☐ Gap	☐ N/A
☐	A.8.22	Trennung Produktion, Test, Entwicklung technisch durchgesetzt	☐ Ready	☐ Gap	☐ N/A
☐	A.8.24	Kryptographie-Richtlinie mit zugelassenen Algorithmen	☐ Ready	☐ Gap	☐ N/A
☐	A.8.25	Sicherer SDLC mit Security-Gates im Entwicklungsprozess	☐ Ready	☐ Gap	☐ N/A
☐	A.8.28	Secure-Coding-Guidelines, Code-Review-Nachweise	☐ Ready	☐ Gap	☐ N/A
☐	A.8.29	Security-Tests (SAST, DAST) als Teil der Pipeline	☐ Ready	☐ Gap	☐ N/A
☐	A.8.31	Trennung Dev / Test / Prod durchgesetzt und nachweisbar	☐ Ready	☐ Gap	☐ N/A
☐	A.8.32	Change-Management-Historie vollständig, mit Risikobewertung	☐ Ready	☐ Gap	☐ N/A
☐	A.8.34	Schutz von Informationssystemen während interner Audits	☐ Ready	☐ Gap	☐ N/A

Audit-Interviews und Walk-Through

û	Control	Nachweis / Evidence	Status			Evidence Location
☐	Host	Audit-Host benannt (meist CISO oder ISMS-Manager)	☐ Ready	☐ Gap	☐ N/A	
☐	CISO	CISO verfügbar für Fragen zu Klauseln 5, 6, 9 und 10	☐ Ready	☐ Gap	☐ N/A	
☐	IT-Admin	IT-Administrator für Zugriffs- und Netzwerkthemen vorbereitet	☐ Ready	☐ Gap	☐ N/A	
☐	Dev	Entwicklungsleiter für A.8.25 bis A.8.28 verfügbar	☐ Ready	☐ Gap	☐ N/A	
☐	HR	HR-Vertreter für A.6 und Background-Checks verfügbar	☐ Ready	☐ Gap	☐ N/A	
☐	Einkauf	Einkauf / Procurement für A.5.19 bis A.5.22 verfügbar	☐ Ready	☐ Gap	☐ N/A	
☐	Walk	Pre-Audit-Walk-Through 1 Woche vorher mit allen Interviewten	☐ Ready	☐ Gap	☐ N/A	