ISO 27001:2022 · STAGE 1

Stage 1 Readiness Checklist

Documentation Review nach ISO 27001:2022 — 40-Punkte-Check

VERSION
1.0

STAND
6. Oktober 2026

LIZENZ
Creative Commons CC-BY-4.0

OPEN LICENCE · CC-BY-4.0

Diese Vorlage ist unter Creative Commons CC-BY-4.0 lizenziert. Freie Nutzung, Weitergabe und Anpassung erlaubt, mit Nennung: Kopexa GmbH, kopexa.com.

Ausfüllhinweise

Diese Checkliste strukturiert deine Stage-1-Vorbereitung (Documentation Review) nach ISO 27001:2022. Stage 1 prüft, ob deine ISMS-Dokumentation vollständig und normkonform ist. Jede Zeile repräsentiert ein zentrales Prüfdokument. Nutze die Status-Spalte, um die Reifegradabschätzung zu dokumentieren.

Legende

1. Status: Ready = vollständig; Gap = Lücke erkannt; N/A = nicht anwendbar mit Begründung
2. Evidence Location: Pfad, Ticket-ID oder URL zum Dokument
3. Notes: Kurzer Kommentar zum Reifegrad oder zur Zuständigkeit

Diese Vorlage ist CC-BY-4.0 lizenziert. Freie Nutzung mit Nennung: Kopexa GmbH, kopexa.com. Kein Ersatz für Rechtsberatung. ISO 27001:2022 — Stand 2026-04-18.

Klausel 4 — Kontext der Organisation

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	4.1	Interne und externe Themen identifiziert und dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	4.2	Interessierte Parteien und ihre Anforderungen erfasst	☐ Ready ☐ Gap ☐ N/A	
☐	4.3	ISMS-Scope-Statement formell verabschiedet, mit Begründung von Ausschlüssen	☐ Ready ☐ Gap ☐ N/A	
☐	4.4	ISMS als Prozessmodell dokumentiert	☐ Ready ☐ Gap ☐ N/A	

Klausel 5 — Führung

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	5.1	Verpflichtungserklärung der Geschäftsführung vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	5.2	Informationssicherheitsrichtlinie freigegeben und kommuniziert	☐ Ready ☐ Gap ☐ N/A	
☐	5.3	Rollen und Verantwortlichkeiten zugewiesen (CISO, ISMS-Manager, interne Auditoren)	☐ Ready ☐ Gap ☐ N/A	

Klausel 6 — Planung

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	6.1.1	Risiken und Chancen beurteilt, Planung zur Behandlung dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	6.1.2	Risikomethodik schriftlich fixiert mit Kriterien für Akzeptanz	☐ Ready ☐ Gap ☐ N/A	
☐	6.1.2	Risikoregister vollständig, mit Owner und Bewertungsstand	☐ Ready ☐ Gap ☐ N/A	
☐	6.1.3 d	Statement of Applicability (SoA) mit allen 93 Annex-A-Controls erstellt	☐ Ready ☐ Gap ☐ N/A	
☐	6.1.3	Risk Treatment Plan mit Maßnahmen, Verantwortlichen und Terminen	☐ Ready ☐ Gap ☐ N/A	
☐	6.2	Informationssicherheitsziele definiert und messbar gemacht	☐ Ready ☐ Gap ☐ N/A	

Klausel 7 — Unterstützung

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	7.1	Ressourcen zur ISMS-Umsetzung bereitgestellt	☐ Ready ☐ Gap ☐ N/A	
☐	7.2	Kompetenznachweis für ISMS-Rollen dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	7.3	Awareness-Maßnahmen durchgeführt und dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	7.4	Kommunikationsplan für interne und externe Kommunikation vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	7.5	Dokumentenlenkung etabliert (Versionierung, Freigabe, Aufbewahrung)	☐ Ready ☐ Gap ☐ N/A	

û	Ref.	Dokument / Nachweis	Status	Evidence Location

Klausel 8 — Betrieb

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	8.1	Betriebliche Planung und Steuerung dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	8.2	Mindestens ein durchgeführter Risk-Assessment-Zyklus	☐ Ready ☐ Gap ☐ N/A	
☐	8.3	Risikobehandlungs-Umsetzung begonnen und nachweisbar	☐ Ready ☐ Gap ☐ N/A	

Klausel 9 — Bewertung der Leistung

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	9.1	KPIs für Überwachung und Messung definiert	☐ Ready ☐ Gap ☐ N/A	
☐	9.2	Internal Audit Plan freigegeben, mindestens ein Audit durchgeführt	☐ Ready ☐ Gap ☐ N/A	
☐	9.2	Interner Auditbericht mit Findings vorhanden	☐ Ready ☐ Gap ☐ N/A	
☐	9.3	Mindestens ein Management-Review-Zyklus vollständig protokolliert	☐ Ready ☐ Gap ☐ N/A	

Klausel 10 — Verbesserung

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	10.1	Nonconformity- und Corrective-Action-Prozess dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	10.1	Mindestens eine geschlossene Nonconformity mit Wirksamkeitsprüfung	☐ Ready ☐ Gap ☐ N/A	
☐	10.2	Kontinuierliche Verbesserung nachweisbar (Lessons Learned, KVP-Tickets)	☐ Ready ☐ Gap ☐ N/A	

Annex A — Dokumentationsvoraussetzungen

û	Ref.	Dokument / Nachweis	Status	Evidence Location
☐	A.5.1	Informationssicherheitsrichtlinien freigegeben und verteilt	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.2	Rollen und Verantwortlichkeiten formal zugewiesen	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.9	Asset-Inventory vollständig mit Owner und Klassifizierung	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.19	Lieferantenregister mit Risikobewertung für kritische Dienstleister	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.24	Incident-Management-Plan dokumentiert	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.3	Awareness- und Schulungsnachweise aller Mitarbeitenden	☐ Ready ☐ Gap ☐ N/A	
☐	A.6.6	NDA-Vorlagen für Mitarbeitende und Lieferanten	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.13	Backup-Konzept dokumentiert, Restore-Test eingeplant	☐ Ready ☐ Gap ☐ N/A	
☐	A.8.32	Change-Management-Prozess dokumentiert	☐ Ready ☐ Gap ☐ N/A	

CC-BY-4.0 — Kopexa GmbH — Vorlage zur freien Nutzung mit Quellenangabe