

AUDIT-09 — ISO 9001 Klausel-für-Klausel Mapping

Stand: 2026-05-17 **Reife-Skala:** ✓ Etabliert · 🕒 Im Aufbau · ○ Geplant

Klausel	Anforderung	Umsetzung & Beleg	Reife
§4.1	Externe + interne Themen verstehen	Trust-Center ce-doc.eu/sicherheit.html + META_INDEX.md	✓
§4.2	Interessierte Parteien	Mandanten, deren Hersteller-Kunden, CE-Koordinator, Auditoren, Marktüberwachung, Sub-Verarbeiter — siehe rollen_zuordnung.md	✓
§4.3	Anwendungsbereich QMS	siehe 01_scope.md	✓
§4.4	Prozesse	4 Kern-Prozesse PROC-K1 bis PROC-K4 mit I/O, Verantwortung, KPIs	✓
§5.1	Verpflichtung der Leitung	Qualitätspolitik POL-04 verfasst, GF-Unterschrift ausstehend	🕒
§5.2	Qualitätspolitik	POL-04 (5 Verpflichtungen, 7 Qualitätsziele) — Entwurf, formell in Kraft mit GF-Unterschrift	🕒
§5.3	Rollen + Befugnisse	rollen_zuordnung.md mit 8 Rollen + Zugriffs-Matrix	✓
§6.1	Risiken + Chancen	strategy/12_audit_sprint_plan.md mit erwarteten Findings + Audit-Befund-Dashboard	✓
§6.2	Qualitätsziele	POL-04 §3 (7 Ziele) + _KPI_DASHBOARD.md	✓
§6.3	Planung von Änderungen	PROC-K2 Software-Lifecycle (4 Release-Klassen mit Approval-Trail)	✓
§7.1.1	Ressourcen	Hetzner Helsinki/Frankfurt, GPU-Roadmap on-prem, LLM-Provider mit DPAs	✓
§7.1.2	Personen	rollen_zuordnung.md mit Rechtsgrundlage-Status pro Person	🕒 ORG-1

Klausel	Anforderung	Umsetzung & Beleg	Reife
§7.1.3	Infrastruktur	docs/INFRASTRUCTURE.md	✓
§7.1.4	Umgebung	Cloud-Hosting + Home-Office, keine kritische physische Umgebung	✓
§7.1.5	Überwachungsmittel	LLM-Drift-Check, Eval-Korpus, Health-Endpoint, Static-Security-Check	✓
§7.1.6	Wissen	Wissensbasis-Lookups + Norm-Pool + Doku-Tree	✓
§7.2	Kompetenz	Kompetenz-Anforderungen pro Rolle in rollen_zuordnung.md, individuelle Lebensläufe separat	●
§7.3	Bewusstsein	jährliche schriftliche „gelesen-und-verstanden“-Bestätigung pro Rolle, Verfahren etabliert	● erste Runde noch ausstehend
§7.4	Kommunikation	Trust-Center extern, Portal intern, Mail-Kanäle für Koordinator	✓
§7.5	Dokumentierte Information	governance/-Struktur mit Versions-Stempeln pro Lookup-Datei, Git als Lenkungssystem	✓
§8.1	Planung + Steuerung	PROC-K1 Schritt-Schema	✓
§8.2	Kunden-Anforderungen	PROC-K1 Onboarding mit Pre-Vertrags-Phase + Klärungs-Pfad	✓
§8.3	Design + Entwicklung (Software)	PROC-K2 Release-Klassen + CI-Tests + Eval-Korpus als V&V	✓
§8.4	Externe Anbieter	PROC-K4 Anbieter-Bewertung + Sub-Verarbeiter-Liste + DPAs	✓
§8.5.1	Steuerung der Erbringung	PROC-K1 + Health-Endpoint + Pipeline-Telemetrie	✓
§8.5.2	Identifikation + Rückverfolgbarkeit	CM-1 Konfigurations-Stempel SHA-256, LW-1 Lookup-First-Prinzip	✓
§8.5.3	Eigentum von Kunden	Tenant-isolierte Workspaces, kein Training auf Mandanten-Daten, AVV-Vertrag	✓
§8.5.4	Erhaltung	Backup mit Retention; in-transit verschlüsselt ✓, at-rest in Arbeit (AUD-5)	●
§8.5.5			✓

Klausel	Anforderung	Umsetzung & Beleg	Reife
	Tätigkeiten nach Lieferung	Klärungs-Schleifen + 10-Jahres-Akten-Archiv (PROC-K3)	
§8.5.6	Änderungen während Erbringung	VAL-11 Akte-Re-Reader + VAL-12 Carry-Over + Lifecycle-Wache	✓
§8.6	Freigabe	FG-1 Freigabe-Gate + Vier-Augen-Prinzip + Koordinator-Identität in Sektion 22	✓
§8.7	Nichtkonforme Outputs	OPL-Lebenszyklus + PROC-K3 Incident-Response	✓
§9.1.1	Überwachung + Messung	_KPI_DASHBOARD.md mit 10 zentralen KPIs aus 4 Kern-Prozessen	✓
§9.1.2	Kundenzufriedenheit	Pilot-Koordinator-NPS-Verfahren definiert (Quartals-Kurz-Umfrage)	○ erste Erhebung mit erstem Pilot-Mandant
§9.1.3	Analyse + Bewertung	im Management-Review jährlich + KPI-Schwellen-Alerts	●
§9.2	Internes Audit	PROC-K4 + 11 Audit-Bündel + Audit-Kalender	✓
§9.3	Management-Review	_MANAGEMENT_REVIEW.md — Initial-Review 2026-05-17 dokumentiert, Folge-Reviews quartalsweise + jährlich	✓
§10.1/10.2	Nichtkonformität + Korrektur	PROC-K3 + Befund-Lifecycle in Audit-Bündeln	✓
§10.3	Fortlaufende Verbesserung	Goel-Okumoto-Reliability-Growth + Audit-Befunde + Post-Mortem-Lessons-Learned	✓

Reife-Übersicht

Status	Anzahl Klauseln	Anteil
✓ Etabliert	29	72,5 %
● Im Aufbau	10	25 %
○ Geplant	1	2,5 %
Summe	40	—

Bewertung: Substantielle Norm-Abdeckung. Lücken konzentriert in §5.1/§5.2 (POL-04-Unterschrift), §7.1.2/§7.2 (Rechtsgrundlage Philipp), §7.3 (erstmalige Bewusstseins-Bestätigungen), §8.5.4 (at-rest-Verschlüsselung) und §9.1.2 (NPS-Erhebung mit erstem Pilot). Mitigations-Roadmap siehe [04_findings.md](#) . Belege je Klausel siehe [03_evidence.md](#) .