

PROC-K4 — Audit & Verbesserung

Verantwortlich: R-COMP **Bezugsnormen:** ISO 9001 §8.4, §9.2, §9.3, §10 · ISO 19011 · ISO 42001 §9.2

Internes Audit-Programm

11 Audit-Aspekte, gestaffelte Frequenz:

Aspekt	Frequenz
AUDIT-04 ISO 25010 Software-Qualität	halbjährlich
AUDIT-05 Verfügbarkeit + Incident-Response	vierteljährlich (mit Restore-Drill)
AUDIT-06 Cross-Provider-Privacy	quartalsweise + bei Provider-AGB-Änderung
AUDIT-01, -02, -03a, -03b, -09	jährlich (DSGVO, OWASP, ISO 42001, NIST AI RMF, ISO 9001)
AUDIT-07 Pentest	halbjährlich intern + jährlich extern (R-EXT-AUD)
AUDIT-08 DPIA	pro Pilot-Mandant + jährlich
AUDIT-10 ISO 14001	jährlich, leichtgewichtig

Jeder Audit-Lauf folgt der Datei-Konvention im jeweiligen `audits/AUDIT-XX/` -Bündel (Policy, Scope, Controls, Findings, Review-Log).

Externe Audits: Mindestens 2 von 11 Aspekten jährlich extern. 2026: Pentest (extern Q3) + ISO 9001 Coaching-Audit durch Vater.

Familien-Audit-Beziehung wird transparent dokumentiert und nicht als „unabhängig“ deklariert.

Anbieter-Bewertung (§8.4)

Sub-Verarbeiter (Hetzner, Mistral, Anthropic, Mailbox.org, Ionos) werden jährlich neu bewertet gegen 7 Kriterien:

Kriterium	Gewicht
Vertragliche Substanz (DPA, SCC, No-Training)	25 %

Kriterium	Gewicht
Hosting-Standort (EU bevorzugt)	20 %
Zertifikate	15 %
Technische Eignung	15 %
Wirtschaftlichkeit	10 %
Reputation / Insolvenz-Risiko	10 %
Exit-Strategie	5 %

Schwelle $\geq 3,5 / 5$. Bewertungstabelle in `audits/AUDIT-06_cross_provider_privacy/`.

Befund-Management

Befunde werden mit Schwere klassifiziert und im zentralen Dashboard `audits/BEFUND_DASHBOARD.md` verfolgt:

Schwere	Termin zur Schließung
HIGH	90 Tage
MED	180 Tage
LOW	nächster Audit-Zyklus

Geschlossene Befunde bleiben append-only im Audit-Trail.

Management-Review (§9.3)

Mindestens jährlich, dokumentiert in `audits/_MANAGEMENT_REVIEW.md`. Eingangsgrößen nach §9.3.2: Maßnahmen-Status, Umfeld-Änderungen, Leistung, Kundenzufriedenheit (NPS), Risiken/Chancen, Ressourcen-Bedarf, Verbesserungs-Möglichkeiten. Output: Beschlüsse mit Verantwortlichkeit und Termin.

Kontinuierliche Verbesserung (§10.3)

KVP läuft über drei Quellen: - **Audit-Befunde** mit Mitigations-Roadmap - **Reliability-Growth** (Goel-Okumoto über Sprint-Iterationen, dokumentiert in `docs/analyse_kampagne_2026-05/`) - **Post-Mortem-Lessons-Learned** (PROC-K3)

Records

- Befund-Dashboard (dauerhaft)
- Review-Logs pro Aspekt (dauerhaft, append-only)

- Management-Review-Historie (dauerhaft)
- Anbieter-Register (dauerhaft, Versions-Historie)
- Externe Auditor-Verträge (10 Jahre)

KPI

KPI	Soll
Audit-Plan-Erfüllungsquote	100 %
Externe Audit-Quote	≥ 2 / Jahr
Mittlere HIGH-Befund-Schließungs-Zeit	≤ 90 Tage
Reife-Anstieg pro Aspekt	$\geq +0.2$ / Jahr