

Befund-Dashboard — alle Audit-Aspekte

Stand: 2026-05-17 **Verantwortlich:** R-COMP **Bezug:** PROC-K4 + POL-09 §7 + ISO 9001 §10.2 + ISO 19011 §6.6 **Update-Frequenz:** bei jedem Audit-Lauf + monatlich beim KPI-Review **Konvention:** Append-only. Geschlossene Befunde wandern in den Abschnitt „Geschlossen“, werden nicht gelöscht.

Offene Befunde — Priorität HIGH (Schließung binnen 90 Tagen)

ID	Audit-Aspekt	Klausel	Befund (Kurz)	Maßnahme	Termin	Status
AUDIT-09-F-02	AUDIT-09 ISO 9001	§7.1.2 / §7.2	ORG-1: Hauptverarbeitender ohne formalen Werkvertrag mit EcoHub	Werkvertrags-Konstruktion mit Steuerberater	2026-09-30	offen
AUDIT-09-F-04	AUDIT-09 ISO 9001	§8.5.4	AUD-5: Mandanten-Live-Daten at-rest unverschlüsselt	LUKS / App-Level-Encryption	2026-06-30	offen, KW 24–25 Code-Sprint
AUDIT-01-F-AUD-1	AUDIT-01 DSGVO	Art. 32	PII-Anonymisierung in Logs unvollständig	Log-Anonymisierungs-Filter	2026-06-30	offen, KW 24–25 Code-Sprint
AUDIT-01-F-AUD-8	AUDIT-01 DSGVO	Art. 32 + MV 10J	Archivierungs-Service mit Hash-Stempel fehlt produktiv	Archiv-Service implementieren	2026-06-30	offen, KW 24–25 Code-Sprint
AUDIT-08-F-01	AUDIT-08 DPIA	DSGVO Art. 32	PII-Anonymisierung in Live-Logs unvollständig (Doppel von AUD-1)	gemeinsamer Filter im Logging-Pfad	2026-06-30	offen, KW 24–25
AUDIT-08-F-02	AUDIT-08 DPIA	DSGVO Art. 32	At-rest-Verschlüsselung Workspace-Volume offen (Doppel von AUD-5)	LUKS-Setup	2026-06-30	offen, KW 24–25
				Archiv-Service	2026-06-30	

ID	Audit-Aspekt	Klausel	Befund (Kurz)	Maßnahme	Termin	Status
AUDIT-08-F-03	AUDIT-08 DPIA	DSGVO Art. 32 + MV	Archivierungs-Service offen (Doppel von AUD-8)			offen, KW 24-25
AUDIT-12-F-04	AUDIT-12 Forensik	MV 10-J	10-J-Archiv-Hash-Manifest offen (Doppel von AUD-8)	gekoppelt mit AUD-8	2026-06-30	offen, KW 24-25
POL-10-F-01	POL-10 Haftung	Pilot-Vertrag	EcoHub-eigene Cyber + Betriebshaftpflicht-Versicherung noch nicht abgeschlossen	Versicherungs-Recherche + Abschluss	Q3 2026	offen, vor erstem Pilot zwingend
BCM-F-01	strategy/ 13 BCM	ISO 22301	Code-Escrow-Vertrag nicht abgeschlossen	Treuhänder kontaktieren + Vertrag	Q3 2026	offen, vor erstem Pilot zwingend

Offene Befunde — Priorität MED (Schließung binnen 180 Tagen)

ID	Audit-Aspekt	Klausel	Befund (Kurz)	Maßnahme	Termin	Status
AUDIT-09-F-01	AUDIT-09 ISO 9001	§5.2	Qualitätspolitik POL-04 noch nicht unterzeichnet	GF-Unterschrift-Termin	2026-05-31	offen
AUDIT-09-F-07	AUDIT-09 ISO 9001	§7.2	„Interner Auditor ISO 9001/42001“-Zertifikat R-AUD fehlt	TÜV/IHK-Schulung Q3 2026	2026-09-30	offen
AUDIT-09-NC-EXT-05	AUDIT-09 ISO 9001	ISO 19011 §5	POL-09 §5 vs §6.4: Familien-Audit als „extern“ gelistet aber „nicht-unabhängig“ deklariert (Widerspruch)	POL-09 §5 begrifflich auf „strukturierter externer Review nicht-unabhängig“ splitten, KPI splitten	2026-09-30	offen
AUDIT-11-F-02	AUDIT-11 Multi-Tenant	OWASP ASVS V5.1.5	Path-Traversal mit Sonderzeichen-codiertem case_id	case_id-Regex-Validator	2026-06-30	offen
AUDIT-11-F-03		DSGVO Art. 32		gekoppelt mit AUD-1	2026-06-30	offen

ID	Audit-Aspekt	Klausel	Befund (Kurz)	Maßnahme	Termin	Status
	AUDIT-11 Multi-Tenant		Pipeline-Logs enthalten unanonymisierte PII (gekoppelt mit AUD-1)			
AUDIT-12-F-01	AUDIT-12 Forensik	ISO 9001 §8.5.2	Lookup-yaml-Hash nicht in akt_state.audit.lookup_versionen gespeichert	Pipeline-Hook in aggregiere_alle	2026-06-30	offen
AUDIT-12-F-03	AUDIT-12 Forensik	ISO 9001 §8.5.2	Modell-Provenance-Vollständigkeits-CI-Gate fehlt	Pytest-Test	2026-06-30	offen
POL-10-F-02	POL-10 Haftung	Pilot-Vertrag	Pilot-Vertrag-Haftungs-Klauseln noch nicht anwaltlich gegengeprüft	Anwalt-Termin	Q3 2026	offen
BCM-F-02	strategy/13 BCM	Notfall	Notfall-Vorsorge-Vollmacht GF nur informell	Notar-Termin	Q3 2026	offen
BCM-F-03	strategy/13 BCM	IP-Trennung	Open-Source-Pfad-Bewertung der IP-Kern-Trennung	IP-Analyse	Q3 2026	offen

Offene Befunde – Priorität LOW (Schließung im nächsten Audit-Zyklus)

ID	Audit-Aspekt	Klausel	Befund (Kurz)	Maßnahme	Termin	Status
AUDIT-09-F-03	AUDIT-09 ISO 9001	§7.3	Erstmalige schriftliche „gelesen-und-verstanden“-Bestätigung der Qualitätspolitik	nach POL-04-Unterschrift einholen	2026-06-30	offen
AUDIT-09-F-05	AUDIT-09 ISO 9001	§9.1.2	NPS-Erst-Erhebung mit erstem Pilot-Mandanten	mit Pilot-Vertrag aktivieren	Q3 2026	offen
AUDIT-09-F-06	AUDIT-09 ISO 9001	§9.3	Quartals-Mini-Review-Folgetermin	Kalender-Eintrag 2026-08-17	2026-08-17	offen
AUDIT-09-F-08	AUDIT-09 ISO 9001	§7.2	DSGVO-Praktiker-Zertifikat R-GF fehlt	DSGVO-Schulung Q3 2026	2026-09-30	offen

ID	Audit-Aspekt	Klausel	Befund (Kurz)	Maßnahme	Termin	Status
AUDIT-09-NC-EXT-08	AUDIT-09 ISO 9001	§7.5	URL-Belegketten ce-doc.eu vs aimos-industrial.de nicht eindeutig	URLs verifizieren + Doku- Anpassung	2026-05-24	offen
AUDIT-08-F-04	AUDIT-08 DPIA	DSGVO Art. 28	Quartalsweises Provider-AGB- Audit- Verfahren Erst- Durchführung Q3 2026	PROC-K2 Termin setzen	2026-09-30	offen
AUDIT-08-F-05	AUDIT-08 DPIA	DSGVO Art. 33	Datenpannen- Tabletop-Drill ausstehend	mit Quartals-DR- Drill koppeln	2026-08-17	offen
AUDIT-08-F-06	AUDIT-08 DPIA	Koordinator- Vorlage	DPIA-Vorlage Pilot- Validierung steht aus	mit erstem Pilot- Koordinator durchspielen	Q3 2026	offen
AUDIT-11-F-04	AUDIT-11 Multi-Tenant	Konzeptionell	Session-Token ohne separaten berater_id- Claim	Token- Schema erweitern	KW 28 2026	offen
AUDIT-12-F-02	AUDIT-12 Forensik	MV 10-J	Pro Pilot-Akte fehlt expliziter Git-Tag	git-Tag- Konvention in FG-1	KW 28 2026	offen
POL-10-F-03	POL-10 Haftung	Pitch	Versicherungs- Empfehlung an Koordinator im Pitch-Material aufnehmen	Pitch-Slide ergänzen	KW 22 2026	offen
BCM-F-04	strategy/ 13 BCM	Pilot-Vertrag	90-Tage- Vorlauf-Klausel im Pilot- Vertrag ergänzen	Vertrags- Edit	KW 22 2026	offen

Stage-1-Audit-Erwartungen (vor Audit-Sprint noch nicht erhoben)

Stand 2026-05-17: für AUDIT-01 (DSGVO), AUDIT-02 (OWASP), AUDIT-07 (Pentest), AUDIT-08 (DPIA) liegen vorläufige Erwartungen aus Strategy/12 vor — konkrete Befund-IDs werden erst im jeweiligen Audit-Lauf vergeben:

Audit-Aspekt	Erwartete HIGH	Erwartete MED	Erwartete LOW
AUDIT-01 DSGVO TOM	~2	~3	~3
AUDIT-02 OWASP ASVS L2	~1	~3	~5
AUDIT-07 Pentest extern	wird Q3 2026 mit Anbieter erhoben	dito	dito
AUDIT-08 DPIA	~1	~4	~4
AUDIT-03a/-03b/-04/-05/-06/-10	wird im jeweiligen Audit-Lauf erhoben	dito	dito

→ Quelle: docs/governance/strategy/12_audit_sprint_plan.md . Diese Zahlen sind Schätzungen, keine Befund-Belegung. Konkrete Belege erst nach durchgeführtem Audit-Lauf.

Geschlossene Befunde (Audit-Trail, append-only)

ID	Geschlossen am	Audit-Aspekt	Befund	Verifikation
AUDIT-09-NC-EXT-01	2026-05-17	AUDIT-09	03_evidence.md fehlte	Datei angelegt mit Klausel-Mapping §4-§10
AUDIT-09-NC-EXT-02	2026-05-17	AUDIT-09	_BEFUND_DASHBOARD.md fehlte	dieses File angelegt
AUDIT-09-NC-EXT-03	2026-05-17	AUDIT-09	Inkonsistenz „8 vs. 11 Audit-Aspekte“ in POL-04, POL-09, README, Management-Review	Sweep auf „11“ durchgeführt, alle Top-Level-Dokumente synchronisiert
AUDIT-09-NC-EXT-04	2026-05-17	AUDIT-09	§5.2-Reife in 02_controls.md inkohärent („✓ (🔴 Unterschrift)“)	Bewertung auf 🔴 korrigiert, Tabellen-Summe nachgezogen
	2026-05-17	AUDIT-09		

ID	Geschlossen am	Audit-Aspekt	Befund	Verifikation
AUDIT-09-NC-EXT-06			README AUDIT-09 sagte „Vier“ Dateien, listete fünf	Text auf „Fünf bzw. nach Kanon-Vollständigkeit sechs“ angepasst
AUDIT-09-NC-EXT-07	2026-05-17	AUDIT-09	governance/README.md veralteter Bündel-Range „AUDIT-01 bis AUDIT-08“	auf „AUDIT-01 bis AUDIT-10 (mit -03a/-03b)“ aktualisiert
AUDIT-11-F-01	2026-05-18	AUDIT-11 Multi-Tenant	HIGH — Vorgangs-Endpoints prüfen Koordinator-Tenant nicht; Koordinator A konnte via case_id-URL-Manipulation auf Daten von Koordinator B zugreifen	<code>_assert_tenant</code> -Helper + <code>_lade_state(case_id, request)</code> + Listen-Filter in 13 HTTP-Endpoints (<code>cedoc-portal/backend/api.py</code>); Pytest 9/9 grün (<code>tests/test_portal_tenant_isolation.py</code>); Same-Day-Fix nach Initial-Audit

Eskalations-Logik

Befunde, die ihren Termin überschreiten, lösen automatische Eskalation aus:

Überschritten um	Eskalations-Stufe
0-14 Tage	R-COMP-Notiz im Monatsbericht
15-30 Tage	R-GF-Information im nächsten Quartals-Review-Vorgriff
> 30 Tage	außerordentliches Management-Review (POL-09 §9 i. V. m. §10.2)

Reife-Status (aggregiert über alle Aspekte)

Aspekt	Reife	letzter Lauf	nächster Lauf
AUDIT-01 DSGVO TOM	🕒 Im Aufbau	KW 21 (Stub)	KW 22
AUDIT-02 OWASP ASVS L2	🕒 Im Aufbau	KW 21 (Stub)	KW 23
AUDIT-03a ISO 42001	✓ Gap-Assessment	2026-05 (ANA-7)	jährlich
AUDIT-03b NIST AI RMF	✓ Self-Check	2026-05 (ANA-7)	jährlich
AUDIT-04 ISO 25010	🕒 Im Aufbau	KW 21 (Stub)	KW 23
AUDIT-05 Verfügbarkeit + IR	🕒 Im Aufbau	KW 21 (Stub)	KW 23

Aspekt	Reife	letzter Lauf	nächster Lauf
AUDIT-06 Cross-Provider-Privacy	● Im Aufbau	KW 21 (Stub)	KW 23
AUDIT-07 Pentest	○ Geplant	n/a	Q3 2026 (extern)
AUDIT-08 DPIA	● Im Aufbau	KW 21 (Stub)	pro Pilot
AUDIT-09 ISO 9001	✓ Initial-Lauf 2026-05-17	2026-05-17 (Self-Assessment + Self-Audit-Of-Self-Audit)	KW 21-23 Coaching
AUDIT-10 ISO 14001 leichtgewichtig	● Im Aufbau	KW 21 (Stub)	jährlich
AUDIT-08 DPIA	✓ Anbieter-DPIA + Koordinator-Vorlage 2026-05-18	2026-05-18	pro Pilot + jährlich
AUDIT-11 Multi-Tenant-Isolation	✓ Initial + Same-Day-Fix 2026-05-18	2026-05-18	KW 47 2026 (halbjährlich)

Stand-Snapshot: 2026-05-17. Befunde aus diesem Dashboard werden in den jeweiligen `audits/AUDIT-XX/04_findings.md` detailliert geführt; hier ist die konsolidierte Sicht für Management-Review und Eskalations-Steuerung.