

AUDIT-09 — Audit-Bericht (Review-Log)

Konvention: Append-only. Jeder Audit-Lauf wird unten angehängt.

Selbst-Audit-Lauf 2026-05-17 — Initial

Auditor: R-COMP (Philipp Fuchsenberger) **Audit-Form:** internes Self-Assessment, vor Coaching-Audit durch externen Auditor **Methodik:** Klausel-für-Klausel-Durchgang ISO 9001:2015 §4 bis §10, anhand der Dokumenten-Belege im governance/-Tree und Code-Stichproben **Dauer:** 3 h Doku-Review + Stichprobenbetrachtung **Status: Self-Assessment, nicht unabhängig** (Auditor ist gleichzeitig Hauptverarbeitender)

1. Audit-Auftrag

Bewertung des Reifegrads des QMS der EcoHub München GmbH (Produktlinie CE-Doc / AIMOS) gegen ISO 9001:2015 zur Vorbereitung eines externen Coaching-Audits.

2. Geltungsbereich

Wie in 01_scope.md festgelegt. Alle Klauseln §4–§10 sind anwendbar mit den dort genannten Anpassungen (§7.1.5 Mess-Mittel ersetzt durch LLM-Drift-Check und Health-Endpoint; §8.3 Design+Entwicklung auf Software-Entwicklung übertragen).

3. Audit-Vorgehen

- Doku-Review: alle Dateien unter docs/governance/ einschließlich Policies, 4 Kern-Prozessen, 11 Audit-Bündeln und Strategie-Dokumenten
- Stichprobenbetrachtung: zwei synth-Workspaces (synth_industrieroboter_240, synth_buehnentechnik_kettenzug_c1) auf Audit-Trail-Lückenlosigkeit
- Cross-Check: Fachstandard, Trust-Center-Seite und Reifegrad-Seite öffentlich verfügbar als Belege

4. Befunde

Siehe 04_findings.md . Zusammenfassung:

Schwere	Anzahl	Bemerkung
HIGH	2	ORG-1 Rechtsgrundlage Mitarbeit, AUD-5 At-rest-Verschlüsselung

Schwere	Anzahl	Bemerkung
MED	2	POL-04-Unterschrift, R-AUD-Zertifikat
LOW	4	Bewusstseins-Bestätigungen, NPS-Erstdurchführung, Q-Review-Folgetermin, R-GF-DSGVO-Zertifikat

5. Bewertung

Konzept-Verständnis: Das QMS folgt durchgängig dem PDCA-Zyklus und ist risiko-basiert. Die 4 Kern-Prozesse decken alle relevanten ISO-9001-Operativen-Klauseln ab. Risiken und Chancen sind im Audit-Sprint-Plan (governance/strategy/12) systematisch erfasst.

Norm-Abdeckung: 30 von 40 untersuchten Klauseln vollständig etabliert (75 %), 9 im Aufbau (22 %), 1 noch ausstehend (3 %, NPS mit erstem Pilot-Mandant).

Substantielle Differenz zu reifen Systemen: Erkennbare Implementierungs- und Formalisierungs-Lücken (ORG-1, AUD-5, POL-04-Unterschrift). Diese sind klar identifiziert, geplant und terminiert. Keine konzeptionellen Lücken im QMS-Aufbau.

Größte Stärken: - Quellen-Bindung jeder Akten-Aussage (LW-1 + CM-1) übertrifft typische Mittelstands-Compliance - 11 Audit-Bündel mit einheitlichem 6-Datei-Kanon ermöglichen systematische externe Audits - Transparente Befund-Dokumentation ohne Optik-Kosmetik

Größte Schwächen: - ORG-1 (HIGH): Rechtsgrundlage Mitarbeit Philipp muss vor erstem produktiven Pilot-Mandanten geklärt sein - AUD-5 (HIGH): At-rest-Verschlüsselung muss umgesetzt sein vor erstem produktiven Pilot-Mandanten - Externe Audit-Unabhängigkeit aktuell nicht gegeben (geplant ab KW 21-23 Coaching-Audit, Q3 2026 externer Pentest)

6. Audit-Schlussfolgerung

Das QMS ist **strukturell vollständig** und **operativ funktionsfähig**. Es ist **nicht zertifizierungs-reif** im Sinne einer ISO-9001-Zertifizierung, aber **audit-fähig** im Sinne eines Coaching-Audits und ausreichend, um vor anspruchsvollen Mandanten-Auditoren die Substanz der Qualitäts-Steuerung zu belegen.

Die identifizierten 8 Befunde sind mit Mitigations-Maßnahmen und Terminen versehen. Bei plangemäßer Umsetzung der HIGH-Findings (ORG-1, AUD-5) bis Q3 2026 ist der Stand „Pilot-tauglich-für-anspruchsvolle-Mandanten“ erreicht.

7. Empfehlungen an die Geschäftsführung

1. **POL-04 unterzeichnen** (sofort wirksam)
2. **Werkvertrag-Konstruktion für Philipp** mit Steuerberater beginnen (Q2/Q3 2026)
3. **Externes Coaching-Audit** durch unabhängigen ISO-9001-Auditor durchführen lassen (geplant KW 21-23)

4. **At-rest-Verschlüsselung** als Code-Sprint vorziehen (KW 24-25)
5. **Quartals-Management-Review** als wiederkehrenden Termin etablieren

8. Nächster Audit-Lauf

- **Coaching-Audit (extern):** KW 21-23 mit Coaching-Auditor
 - **Folge-Self-Audit:** 2027-05-17 (jahresgemäße Wiederholung)
-

Selbst-Audit-Lauf 2026-05-17 — Lauf 2 (Self-Audit-Of-Self-Audit)

Auditor: R-COMP in der Rolle eines simulierten externen Reviewers **Audit-Form:** Konsistenz-Check des Lauf-1-Outputs vor Übergabe an Coaching-Auditor **Methodik:** Datei-Existenz-Check 6-Datei-Kanon + Top-Level-Konsistenz-Check (POL-04, POL-09, governance/README, _KPI_DASHBOARD, _MANAGEMENT_REVIEW, AUDIT-09/) + Logik-Check POL-09 §5 ↔ §6.4 + Reife-Bewertungs-Plausibilität Dauer: 30 min Doku-Sweep + 90 min Mitigation Status: Self-Audit-Of-Self-Audit, nicht unabhängig* — derselbe Auditor, aber bewusst andere Methodik (Konsistenz-Fokus statt Klausel-Fokus)

1. Audit-Auftrag

Prüfung, ob das aus Lauf 1 entstandene Audit-Bündel **vor Übergabe an den Coaching-Auditor (R. Fuchsenberger sen.)** seinem eigenen Anspruch (POL-09 6-Datei-Kanon, konsistente Top-Level-Aussagen) genügt.

2. Methodisches Vorgehen

Schritt	Output
<code>ls</code> auf AUDIT-09_iso9001/ vs POL-09 §3 Kanon	NC-EXT-01: 03_evidence.md fehlt
<code>ls</code> auf audits/ vs PROC-K4 + POL-09 §7	NC-EXT-02: _BEFUND_DASHBOARD.md fehlt
<code>grep -rn "Audit-Aspekt"</code> Quervergleich	NC-EXT-03: 8/11-Inkonsistenz in 6 Dateien
Reife-Skala-Plausibilität in 02_controls.md	NC-EXT-04: §5.2 mit „✓ (🗳 Unterschrift)“ methodisch inkohärent
Innere Logik POL-09 §5 ↔ §6.4	NC-EXT-05: Familien-Audit als „extern“ gelistet + „nicht-unabhängig“ deklariert
README-Lesefluss	NC-EXT-06: „Vier“ vs fünf Dateien

Schritt	Output
governance/README-Bündel-Range	NC-EXT-07: „AUDIT-01 bis AUDIT-08" obwohl AUDIT-09/-10 existieren
URL-Domain-Konsistenz	NC-EXT-08 (offen): ce-doc.eu vs aimos-industrial.de nicht verifiziert

3. Befunde

7 Befunde geschlossen, 1 offen (terminiert 2026-05-24). Details siehe [04_findings.md](#) Abschnitt „Self-Audit-Of-Self-Audit 2026-05-17".

4. Bewertung

Stärke des Lauf-1-Outputs: Klausel-für-Klausel-Tiefe substanziell, Honest Self-Disclosure der Familien-Audit-Beziehung methodisch korrekt, Quellen-Bindung LW-1 + CM-1 über typischem Mittelstand.

Methodische Schwäche, die Lauf 2 entdeckt hat: Lauf 1 ging Klausel-orientiert durch §4-§10, prüfte aber nicht die **Datei-Existenz** der eigenen Kanon-Verweise. Zwei Pflicht-Dateien fehlten unentdeckt — beide hätten der Coaching-Auditor in den ersten 5 Minuten gefunden.

Konsequenz: Self-Audit-Methodik wird für den Folge-Self-Audit-Lauf 2027 um einen Vorabschritt „Datei-Existenz-Check je Kanon-Datei je Aspekt" ergänzt (Aufnahme in PROC-K4 erwägen, ggf. als CI-Test scriptbar).

5. Audit-Schlussfolgerung

Nach den 7 Mitigationen ist das Audit-Bündel **coaching-tauglich**. NC-EXT-08 (URL-Eindeutigkeit) ist vor Coaching-Audit-Termin zu klären, nicht blockierend.

6. Empfehlungen an die Geschäftsführung

1. **POL-04 unterzeichnen** — Top-Level-Kennzahl wurde auf 11 angepasst, daher Re-Unterschrift
2. **PDFs neu rendern** vor Coaching-Audit-Termin
3. **URL-Eindeutigkeit** vor Coaching-Audit klären (M-2026-05-17-16)
4. **Methodik-Update Self-Audit 2027:** Datei-Existenz-Check als Vorabschritt

7. Nächster Audit-Lauf

Identisch zu Lauf 1: - **Coaching-Audit:** KW 21-23 mit R. Fuchsenberger sen. - **Folge-Self-Audit:** 2027-05-17 (mit erweiterter Methodik laut Punkt 4 oben)