

# KI-Nachweise für Kritische Infrastrukturen

*Unabhängige Nachweise für Ihre Risikoanalyse, Ihren Resilienzplan und Ihre EU AI-Act-Konformitätsakte*

---

*Herstellerdokumentation beschreibt, wozu ein System fähig ist. Sie belegt nicht, wie es sich in Ihrem Betriebskontext verhält, gegenüber Ihren Daten, innerhalb Ihres spezifischen Risikobereichs. **Genau diesen Nachweis verlangen NIS2 und der EU AI Act von Ihnen.***

## Die Pflicht gilt jetzt

Mehrere Regulierungsrahmen greifen ineinander und begründen eine verbindliche Nachweispflicht für jede Organisation, die KI in oder im Umfeld kritischer Dienste betreibt.

**DORA** (in Kraft seit Januar 2025): Finanzunternehmen müssen die digitale operative Resilienz ihrer IKT-Systeme nachweisbar sicherstellen — einschließlich Risikomanagement, Incident Reporting und Drittparteirisiken. KI-Systeme, die in Betriebsprozessen oder in der Entscheidungsunterstützung eingesetzt werden, fallen als IKT-Assets in den Geltungsbereich.

**KRITIS-Dachgesetz** (in Kraft seit März 2026): Betreiber kritischer Anlagen müssen innerhalb von neun Monaten nach BBK-Registrierung eine Risikoanalyse abschließen und innerhalb von zehn Monaten einen Resilienzplan umsetzen. KI-Systeme in kritischen Prozessen fallen in den Anwendungsbereich. Die Geschäftsführung haftet persönlich. Bußgelder erreichen bis zu 10 Millionen Euro.

**NIS2 Umsetzungsgesetz** (in Kraft seit Dezember 2025): Pflichten zum Cyber-Risikomanagement und zur Berichterstattung für rund 29.500 Einrichtungen in 18 Sektoren. Soweit KI-Systeme Teil der Leistungserbringung oder der Sicherheitswerkzeuge sind, fällt ihr Verhalten in den Geltungsbereich des Risikomanagements.

**EU AI Act:** Transparenzpflichten gelten ab dem 2. August 2026. Die vollständige Hochrisiko-Regulierung für KI, die im Management und Betrieb kritischer Infrastrukturen eingesetzt wird, gilt ab dem 2. Dezember 2027. Konformität erfordert technische Dokumentation, Nachweise zur Genauigkeit und Robustheit sowie Post-Market-Monitoring.

Herstellerdokumentation beschreibt, wozu ein System fähig ist. Sie belegt nicht, wie

das Systeme sich in Ihrem Betriebskontext verhält, gegenüber Ihren Daten, innerhalb Ihres spezifischen Risikobereichs. Genau diesen Nachweis verlangen KRITIS-Dachgesetz, NIS2 und EU AI Act von Ihnen.

---

## Was Resaro leistet



Resaros KI Assurance Plattform ermöglicht Betreibern kritischer Infrastrukturen, ihre KI-Systeme nach anerkannten Standards zu prüfen und die Ergebnisse regulatorisch verwertbar zu dokumentieren. Resaro ist ein unabhängiges AI-Assurance Venture, gegründet von Temasek, mit Standorten in Singapur und München. Gemeinsam mit unserem Netzwerk aus Industrie-, Forschungs- und Innovationspartnern, darunter die Technische Universität München Venture Labs, treiben wir die Etablierung messbarer Qualitätsstandards und belastbarer Evidenz für vertrauenswürdige KI voran. Wir arbeiten ausschließlich im Interesse der Betreiber — nicht der KI-Anbieter. Als Rapporteur für ETSI TS 104 306 und Beitragender zur ISO-Normierung für LLM-Benchmarking entwickeln wir die methodischen Standards, auf die sich unsere Evaluierungen stützen.

Zwei Elemente bilden die Grundlage unserer Arbeit:

- **ASQI (AI Solutions Quality Index):** ein anwendungsfallspezifisches Qualitätsmessframework, das bei der ETSI als TS 104 306 formal standardisiert wird. ASQI übersetzt einen KI-Anwendungsfall in messbare Qualitätsindikatoren, die direkt auf Ihre regulatorischen Pflichten abgebildet werden.
- **AIP (Approved Intelligence Platform):** führt Testpläne gegen KI-Systeme aus, misst das Systemverhalten anhand von Qualitätsindikatoren und erzeugt reproduzierbare, auditierbare Nachweise.

**ETSI (European Telecommunications Standards Institute)** ist eine der drei offiziellen europäischen Normungsorganisationen und entwickelt technische Standards, die von EU-Regulierung referenziert werden.

### Warum Resaro

- ✓ Rapporteur für ETSI TS 104 306; Beitrag zur ISO-Normierung für LLM-Benchmarking
- ✓ Unabhängig von KI-Anbietern — ausschließlich Betreiberperspektive
- ✓ Prüfung on-premise: Ihre Daten und Systeme verlassen Ihr Haus nicht

## Unser Angebot: ASQI Trial Programme

Ein KI-Anwendungsfall. 6-8 Wochen. Unter EUR 50.000 netto.

| Aktivitäten                       |                                                                                                                                  | Ergebnis                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>AP1:<br/>Use-Case-Workshop</b> | KI-System und Kontext definieren, Qualitätsindikatoren vereinbaren, Pflichten aus KRITIS-Dachgesetz, NIS2 und EU AI Act abbilden | Use Case spezifischer ASQI inkl. regulatorischer Mappings                                             |
| <b>AP2: AIP Evaluation</b>        | Automatisierte Testausführung gegen Ihr KI-System; Messung der Qualitätsindikatoren                                              | Testergebnisse (Qualitätsindikatoren, Qualitätsmaße und deren Werte, Audit Trail durch Evidenz Vault) |
| <b>AP3: ASQI-Bericht</b>          | Vorstellung der qualitative und quantitative Testergebnisse mit regulatorischem Anhang, bereit für Ihre Risikoanalyse            | ASQI Report, Resilienzplan inkl. Roadmap und Ihre KI-Act-Konformitätsakte; Management-Briefing        |

Bereits ausführlich geprüfte KI-Systemtypen: LLM-Anwendungen, RAG-Systeme, Objekterkennung, Deepfake-Detektoren, Foundation-Model-Evaluierungen.

Das Trial-Honorar entspricht den Vorgaben des Vergabebeschleunigungsgesetzes. Öffentliche Auftraggeber können diesen Auftrag ohne förmliches Vergabeverfahren erteilen.

Ihr 25-Minuten-Gespräch — [Terminbuchung](#) — [kritis@resaro.ai](mailto:kritis@resaro.ai)