ENKIDU

— MIOVSKI GROUP —

KONZEPTARCHITEKTUR

Aegis Assure

Ein normenorientiertes Framework zur Bewertung und Akkreditierung von Daten-Governance und -Ethik über den Lebenszyklus von KI-, Machine-Learning- und neuronalen Systemen — geliefert als Dienst der Miovski Group, gegründet auf der Vertrauensdisziplin von Origi.

Deutsch · Kompaktausgabe

Nach Version 0.1 · 4. Juli 2026
Erstellt von MIOVSKI GROUP
Einstufung · Vertraulich · Entwurf zur Weitergabe an Kunden
Die vollständige englische Ausgabe ist maßgeblich

Zu dieser Ausgabe

Dieses Dokument ist eine deutsche Kompaktausgabe von « Aegis Assure — AI Data Ethics Assessment », Version 0.1 (4. Juli 2026), erstellt von der Miovski Group. Jeder Abschnitt des Originals ist in gekürzter Form vertreten. Bei Abweichungen ist die vollständige englische Ausgabe maßgeblich. Einstufung: vertraulich — Entwurf zur Weitergabe an Kunden.

Zusammenfassung

Jede Organisation, die KI einsetzt, sieht sich heute derselben Forderung von Regulierern, Aufsichtsräten, Prüfern und Kunden gegenüber: nicht Funktioniert das Modell?", sondern Können Sie beweisen, dass die Daten dahinter verantwortungsvoll gesteuert wurden?". Die Frage ist schwer zu beantworten, weil die Belege über einen Datenlebenszyklus verstreut sind, den wenige Organisationen je kartiert haben — Beschaffung, Aufnahme, Integration, Klassifizierung, Speicherung, Pflege, Betrieb, Weitergabe, Archivierung und Aussonderung — und weil sich die Normen, die eine gute Antwort definieren, in den letzten achtzehn Monaten stark verschoben haben.

Aegis Assure ist der Dienst der Miovski Group, diese Frage rigoros zu beantworten: ein normenorientiertes Bewertungs- und Akkreditierungsframework aus dreiundsechzig Kriterien über den gesamten Datenlebenszyklus, die unterschiedlichen Pflichten von Trainings- gegenüber Inferenzdaten und die organisatorische Governance darüber. Jedes Kriterium paart eine definierte Nachweispflicht für Praktiker mit strukturierter Anleitung für unabhängige Prüfer, bewertet auf einer Rot-Gelb-Grün-Skala und nach Kritikalität gewichtet — sodass das Ergebnis keine Meinung ist, sondern ein verteidigbares, reproduzierbares Akkreditierungsdossier.

Diese Ausgabe formatiert das zugrundeliegende Framework neu und validiert es erneut. Sie korrigiert das regulatorische Fundament auf den Stand Mitte 2026 — eine Landschaft, die sich seit der Erstfassung wesentlich verändert hat: Kanadas AIDA ist im Parlament gestorben, die EU-KI-Verordnung ist vom Text zu einem gestuften Compliance-Kalender übergegangen, und die Vereinigten Staaten haben ihre Bundeshaltung zweimal umgekehrt. Und sie verortet das Framework an seinem Platz im Enkidu-Stack: als die Governance- und Ethik-Assurance-Schicht, die Origi ergänzt — dieselbe Assurance-Case-Struktur, dieselbe Funktionstrennung, dieselbe Überzeugung, dass eine Behauptung nur so viel wert ist wie die Beweiskette dahinter.

Vertrauen in ein KI-System ist kein Slogan, den man verkündet; es ist eine Position, die man begründet und belegt. Aegis Assure ist, wie diese Position gebaut wird — Kriterium für Kriterium.

1. Dienstüberblick und Positionierung

Aegis Assure ist ein Bewertungs- und Akkreditierungsdienst: Eine Organisation beauftragt die Miovski Group, die Daten-Governance und -Ethik eines oder mehrerer KI-Systeme gegen einen definierten Kriterienkörper zu bewerten und ein Akkreditierungsergebnis zu erzeugen, auf das sich Interessengruppen — Regulierer, Aufsichtsräte, Beschaffungsstellen, Versicherer, Kunden — verlassen können. Das Framework ist das Instrument; der Dienst ist die Lieferung vertrauenswürdiger Befunde durch es. Er gilt für jede Organisation, die KI-Systeme entwirft, entwickelt, einsetzt oder betreibt — mit besonderem Gewicht bei Hochrisiko- und hochwirksamen Anwendungen.

Warum jetzt: Drei Kräfte konvergieren. Die Regulierung hat sich verhärtet — die Hochrisiko- und GPAI-Pflichten der EU-KI-Verordnung folgen nun einem konkreten Kalender. Die Beweislatte ist gestiegen — wir nehmen Ethik ernst" ist keine akzeptable Antwort mehr; verlangt wird dokumentierte, kriterienweise, unabhängig geprüfte Evidenz. Und die Normen selbst haben sich bewegt — viel bestehende Governance-Dokumentation ist veraltet.

- Tangram — Wo findet Arbeit statt, und unter welchen Randbedingungen? — Intern: wie wir bauen.
- Origi — Darf diese Handlung geschehen, und können wir beweisen, was geschah? — Intern: wie wir bauen.
- Helios Grid — Ist das Gewebe gesund, aktuell und wiederherstellbar? — Intern: wie wir bauen.
- Aegis Defence — Überstehen jeder Schlüssel und jede Signatur einen Quantengegner? — Intern: wie wir bauen.
- Aegis Assure — Ist die KI-Daten-Governance dieser Organisation verantwortungsvoll und verteidigbar? — Nach außen: ein Dienst, den wir liefern.

Die Benennung ist bewusst: Aegis Defence schützt die Daten in Bewegung kryptografisch; Aegis Assure schützt die Organisation, indem es beweist, dass ihre Daten ethisch gesteuert wurden. Zwei Schilde — einer technisch, einer beweisführend. Origi und Aegis Assure sind dieselbe Philosophie in zwei Reichweiten: Origi ist ein Laufzeit-Vertrauensgeschirr, das jede Handlung eines laufenden Systems gegen Richtlinien prüft; Aegis Assure ist ein Lebenszyklus-Assurance-Framework, das jede Stufe der Daten-Governance gegen Kriterien prüft — periodisch und zur Akkreditierung. Eine unter Aegis Assure gesicherte Organisation ist gut vorbereitet, Origi zu übernehmen; eine Organisation, die Origi betreibt, erzeugt einen Großteil der von Aegis Assure verlangten Evidenz als Nebenprodukt. Sie sind zum Zusammenwirken entworfen.

2. Regulatorisches Fundament

Das Framework ist bewusst an anerkannten Regimen ausgerichtet, damit seine Ergebnisse nach außen verteidigbar sind — und diese Ausrichtung folgt einer Landschaft, die sich wesentlich verändert hat. Europäische Union: Die KI-Verordnung (Verordnung (EU) 2024/1689) trat am 1. August 2024 in Kraft und gilt gestuft — Verbote und KI-Kompetenzpflichten seit dem 2. Februar 2025; Governance- und GPAI-Pflichten seit dem 2. August 2025; allgemeine Anwendung einschließlich der meisten Hochrisikopflichten am 2. August 2026; eingebettete Hochrisikosysteme am 2. August 2027.

Kanada: Der frühere Verweis auf AIDA als vorgeschlagenen Rahmen" ist nicht mehr aktuell — Bill C-27 starb mit der Prorogation im Januar 2025, und Kanada hat derzeit kein eigenes Bundes-KI-Gesetz. Vereinigte Staaten: EO 14110 wurde im Januar 2025 aufgehoben und durch EO 14179 ersetzt, die die Bundespolitik von Risiko und Rechten zu Innovation und Wettbewerbsfähigkeit umlenkt. Unter den wandernden Statuten liegen die stabilen Normen, die das technische Rückgrat des Frameworks bilden: NIST AI RMF 1.0 samt Generative-AI-Profil, ISO/IEC 42001 und 23894, die DSGVO und ihre Pendants — vor förmlicher Nutzung gegen die offiziellen Publikationen zu bestätigen.

3. Struktur des Frameworks

Das Framework ordnet dreiundsechzig einzigartige Kriterien in drei Teile, einer einzigen Einsicht folgend: Governance-Pflichten unterscheiden sich nach Lebenszyklusstufe, danach, ob die Daten das Modell trainieren oder betreiben, und danach, ob die Kontrolle technisch oder organisatorisch ist.

- Teil A — Datenlebenszyklus — zehn Stufen von der Beschaffung bis zur Aussonderung, bewertet für Trainings- und Inferenzdaten — 41 Kriterien.
- Teil B — Datenbetrieb — geteilt in Trainings- und Inferenzbetrieb, dieselben fünf Kriteriencodes je Phase unterschiedlich angewandt — 10 Kriterien.
- Teil C — Governance und Ethik — organisationsweite Querschnittskriterien, keinem Einzelprojekt zugeordnet — 12 Kriterien.

Die zentrale Strukturdisziplin: Trainings- und Inferenzdaten tragen unterschiedliche Pflichten selbst unter demselben Code — Training wirft Herkunft, Einwilligungsreichweite, historische Verzerrungen und Urheberrecht der Quellen auf; Inferenz wirft Echtzeitvalidierung sowie adversariale und verteilungsfremde Eingaben auf. Jedes Kriterium steht in der Zwei-Rollen-Form, die dem Framework seine Strenge gibt: eine Nachweispflicht, die der Praktiker erfüllen muss, und eine Prüfanleitung, mit der sie beurteilt wird — dieselbe Trennung erst Belege, dann Urteil", die Origi zur Laufzeit erzwingt.

4. Teil A — Die Lebenszyklus-Kriterien

Zehn Stufen tragen einundvierzig Kriterien. Jede benennt ihren Umfang, ihre anwendbare Phase und die Anliegen, die ihre Kriterien bewerten — die Codes bleiben zur Rückverfolgbarkeit ins Bewertungsarbeitsbuch erhalten.

- Beschaffung (AC-01…05) — Rechtsgrundlage der Erhebung (DSGVO Art. 6 / PIPEDA / CCPA), Herkunft und Beweiskette, Erhebungsverzerrung, Datenminimierung, geistiges Eigentum.
- Aufnahme (IN-01…04) — Qualitätsvalidierung, Formatstandardisierung, Sicherheit bei der Aufnahme (Transportverschlüsselung, Authentifizierung, Protokollierung), Label-Qualität.
- Integration (IT-01…04) — End-zu-End-Lineage, quellenübergreifende Qualität, Bewertung der Bias-Verstärkung, Integrations-Governance.
- Klassifizierung (CL-01…04) — Sensitivität (PII/PHI, besondere Kategorien nach Art. 9 DSGVO), regulatorische Einordnung, Training/Inferenz-Kennzeichnung, Zugriffsausrichtung.
- Speicherung (ST-01…05) — Sicherheitskontrollen im Ruhezustand (AES-256, Schlüsselverwaltung, RBAC/ABAC), Aufbewahrung, Sicherung und Wiederherstellung, Prüfprotokolle, Resilienz.
- Pflege (MA-01…05) — Aktualität, Bereinigung und Korrektur, Rebalancierung und Augmentierung, Schemaevolution, fortlaufende Integrität.
- Weitergabe und Verbreitung (SH-01…05, nur Inferenz) — Weitergabe-Governance, Privatsphärenschutz (Anonymisierung, Differential Privacy), Auftragsverarbeiter-Management, Zweckbindung.
- Archivierung (AR-01…04) — Richtlinie und Verfahren, langfristige Sicherheit und Privatsphäre, Dokumentation und Metadaten, dauerhafte Zugänglichkeit (Formatmigration).
- Aussonderung (DR-01…05) — sichere Löschung (kryptografisches Löschen, über alle Speicherorte), Recht auf Löschung, Modellstilllegung, Aussonderungsdokumentation.

5. Teil B — Die Betriebskriterien

Fünf Kriterien (OP-01…05) werden zweimal bewertet — einmal für die Trainingsphase, einmal für die Inferenz — weil sich dasselbe Anliegen in jeder anders verhält: Qualitäts- und Driftüberwachung, Leistungsüberwachung, menschliche Aufsicht, Bias und Fairness, Echtzeitvalidierung. Die inferenzseitigen OP-Kriterien sind der direkteste Treffpunkt von Aegis Assure und Origi: OP-03 (menschliche Aufsicht), OP-04 (Fairness) und OP-05 (adversariale und OOD-Erkennung) beschreiben in Bewertungsbegriffen genau die Prüfungen, die Origis Vertrauensgeschirr zur Inferenzzeit als Durchsetzung ausführt. Eine Organisation, die Origi betreibt, erzeugt die von diesen Kriterien verlangte Evidenz als Betriebsausgabe.

6. Teil C — Governance und Ethik

Zwölf organisatorische Kriterien gelten für jedes System und jede Datennutzung — sie bewerten institutionelle Reife, kein Einzelprojekt.

- Organisatorische Governance (GV-01…03) — KI-Governance-Struktur (Ethikgremium, Aufsicht auf Vorstandsebene), Risikomanagement nach NIST AI RMF, Compliance-Management.
- Dokumentation und Transparenz (DC-01…03) — technische Dokumentation (Model Cards, Dataset Cards), Erklärbarkeit und Interpretierbarkeit (XAI), algorithmische Folgenabschätzungen.
- Ethische Grundsätze und Rechenschaft (ET-01…04) — Fairness und Nichtdiskriminierung, Transparenz und Rechenschaft (Einspruch und Anfechtung), Menschenrechtswirkung, gesellschaftliches Wohl.
- Schulung und Bewusstsein (TR-01…02) — Schulung und Kompetenz des Personals, Organisationskultur (Hinweisgebermechanismen, Vorbild der Führung).

7. Bewertungsmethodik

Die Integrität der Methode ruht auf Funktionstrennung: Praktiker sammeln und dokumentieren die Evidenz je anwendbarem Kriterium; Prüfer bewerten sie unabhängig und vergeben die Noten. Niemand erzeugt und beurteilt zugleich die Evidenz desselben Kriteriums — Origis Trennungsprinzip, auf die Bewertung angewandt.

- Grau — noch nicht bewertet — der Ausgangszustand.
- Grün — konform — die Kontrollen wirken, die Evidenz stützt die Behauptung.
- Gelb — teilweise / kleinere Lücken — Kontrollen existieren, tragen aber kleinere Entwurfs- oder Betriebsmängel.
- Rot — nicht konform — Kontrollen fehlen, wirken nicht oder versagen erheblich.
- Kritisch (C) — 40 % — ein unterschwelliges kritisches Kriterium blockiert die Akkreditierung bis zur Behebung.
- Hoch (H) — 30 % — verlangt einen Behebungsplan vor der Akkreditierung.
- Mittel (M) — 20 % — löst eine Verbesserungs-Roadmap aus.
- Niedrig (L) — 10 % — Fokus kontinuierlicher Verbesserung.

Die Sperrregel ist der Punkt: Ein guter Durchschnitt kauft sich nicht an einer gescheiterten kritischen Kontrolle vorbei — das Spiegelbild von Origis Fail-Closed-Haltung. Und die Ausgabe eines Mandats ist keine Note, sondern ein Dossier: je Kriterium seine Anwendbarkeit, seine Evidenz, die Begründung des Prüfers, seine RGG-Bewertung und sein Behebungsstand — zusammengesetzt zu einer Akkreditierung auf Systemebene mit verteidigbarem Prüfpfad. In Origis Sprache ist dieses Dossier der Assurance-Case der Daten-Governance des Systems.

8. Umsetzung und Lieferung

Praktiker-Workflow: Abgrenzung -> Planung -> Evidenzsammlung (Dokumentation, Interviews, Systemtests) -> Dokumentation -> Lückenidentifikation -> Qualitäts-Eigenprüfung -> Einreichung. Prüfer-Workflow: Evidenzdurchsicht -> Verifikation (Stichproben, Tests, Interviews) -> RGG-Bewertung -> Befunddokumentation -> Kalibrierung im Kollegenkreis -> Bericht (das Akkreditierungsdossier) -> Nachverfolgung der Behebung.

Akkreditierung ist eine zu haltende Position, kein abzuheftendes Zertifikat. Neubewertung wird ausgelöst durch: jährliche Prüfung aller eingesetzten Hochrisikosysteme; wesentliche Systemänderung (neue Datenquellen, Algorithmuswechsel, Nutzungsausweitung); regulatorische Änderung; erhebliche Vorfälle oder Bias-Funde; Übergang vom Pilot in die Produktion. Die Miovski Group liefert den Dienst in drei Formen: eine Bereitschaftsbewertung (schneller Lückenscan, nur RGG), eine vollständige Akkreditierung (der komplette Dreiundsechzig-Kriterien-Zyklus mit Dossier) und kontinuierliche Assurance (wiederkehrende Neubewertung nach dem Auslöserplan, optional mit Origi integriert).

9. Schlussfolgerung

Der Markt ist von der Frage, ob ein KI-System funktioniert, zur Forderung übergegangen, zu beweisen, dass die Daten dahinter verantwortungsvoll gesteuert wurden — und die Normen, die eine gute Antwort definieren, haben sich stark genug verschoben, um viel bestehende Governance-Dokumentation zu veralten, einschließlich der früheren regulatorischen Verweise dieses Frameworks selbst. Diese Ausgabe nimmt die Korrekturen vor: AIDA als gestorben statt anhängig verzeichnet, die EU-KI-Verordnung als lebendiger Stufenkalender statt fernem Text, die US-Haltung als umgekehrt.

Was sich nicht ändert: die Struktur und der Wert des Frameworks — dreiundsechzig Kriterien über den ganzen Lebenszyklus, die Disziplin Training-gegen-Inferenz, die organisatorische Governance darüber und eine Zwei-Rollen-Methode erst Belege, dann Urteil", die ein verteidigbares Akkreditierungsdossier statt einer Meinung erzeugt. Im Enkidu-Stack verortet, ist Aegis Assure das nach außen gewandte Gesicht derselben Vertrauensphilosophie, die Origi im Inneren der Produkte der Miovski Group durchsetzt — der Assurance-Case, die Funktionstrennung, der Vorrang der Evidenz — angeboten als Dienst für jede Organisation, die nun beweisen und nicht bloß behaupten muss, dass ihre KI gut gesteuert ist.

Vertrauen in ein KI-System ist kein Slogan, den man verkündet; es ist eine Position, die man begründet und belegt. Aegis Assure ist, wie diese Position gebaut wird — Kriterium für Kriterium.