



E N K I D U

— M I O V S K I G R O U P —

A R C H I T E C T U R E C O N C E P T U E L L E

Aegis Assure

Un cadre aligné sur les normes pour évaluer et accréditer la gouvernance et l'éthique des données sur tout le cycle de vie des systèmes d'IA, d'apprentissage automatique et de réseaux neuronaux — livré comme service de Miovski Group, ancré dans la discipline de confiance d'Origi.

Français · Édition condensée

D'après la version 0.1 · 4 juillet 2026

Préparé par MIOVSKI GROUP

Classification · Confidentiel · Ébauche pour diffusion aux clients

L'édition anglaise complète fait foi

À propos de cette édition

Ce document est une édition condensée, en français, de « Aegis Assure — AI Data Ethics Assessment », version 0.1 (4 juillet 2026), préparée par Miovski Group. Chaque section de l'original y est représentée sous forme abrégée. En cas de divergence, l'édition anglaise complète fait foi. Classification : confidentiel — ébauche pour diffusion aux clients.

Résumé

Toute organisation qui déploie l'IA fait désormais face à la même exigence de la part des régulateurs, des conseils, des auditeurs et des clients : non pas « le modèle fonctionne-t-il ? » mais « pouvez-vous prouver que les données qui le sous-tendent ont été gouvernées de façon responsable ? ». La question est difficile parce que les preuves sont dispersées sur un cycle de vie des données que peu d'organisations ont jamais cartographié — acquisition, ingestion, intégration, classification, stockage, maintenance, opération, partage, archivage et retrait — et parce que les normes qui définissent une bonne réponse ont fortement bougé au cours des dix-huit derniers mois.

Aegis Assure est le service de Miovski Group pour répondre rigoureusement à cette question. C'est un cadre d'évaluation et d'accréditation aligné sur les normes, fort de soixante-trois critères couvrant l'ensemble du cycle de vie des données, les obligations distinctes des données d'entraînement et d'inférence, et la gouvernance organisationnelle qui les surplombe. Chaque critère associe une exigence de preuves définie pour les praticiens à un guide structuré pour des évaluateurs indépendants, noté sur une échelle Rouge-Ambre-Vert et pondéré par criticité — de sorte que le résultat n'est pas une opinion mais un dossier d'accréditation défendable et reproductible.

Cette édition reformate et revalide le cadre sous-jacent. Elle corrige le socle réglementaire à l'état de la mi-2026 — un paysage matériellement changé depuis la première rédaction : la LIAD canadienne est morte au feuillet, la loi européenne sur l'IA est passée du texte à un calendrier de conformité par phases, et les États-Unis ont inversé deux fois leur posture fédérale. Et elle positionne le cadre à sa place dans la pile Enkidu : la couche d'assurance de la gouvernance et de l'éthique qui complète Origi — même structure de dossier d'assurance, même séparation des devoirs, même conviction qu'une affirmation ne vaut que la chaîne de preuves qui la soutient. Aegis Assure est la manière dont Miovski Group étend vers l'extérieur, comme service, la discipline de confiance qu'il bâtit dans ses propres produits.

La confiance en un système d'IA n'est pas un slogan à proclamer ; c'est une position à argumenter et à prouver. Aegis Assure est la manière dont cette position se construit, critère par critère.

1. Aperçu du service et positionnement

Aegis Assure est un service d'évaluation et d'accréditation : une organisation mandate Miovski Group pour évaluer la gouvernance et l'éthique des données d'un ou plusieurs systèmes d'IA contre un corps défini de critères, et produire un résultat d'accréditation sur lequel les parties prenantes — régulateurs, conseils, autorités d'approvisionnement, assureurs, clients — peuvent s'appuyer. Le cadre est l'instrument ; le service est la livraison de constats dignes de confiance à travers lui. Il s'applique à toute organisation qui conçoit, développe, déploie ou exploite des systèmes d'IA — avec une force particulière pour les applications à haut risque et à fort impact.

Pourquoi maintenant : trois pressions convergent. La réglementation a durci — les obligations à haut risque et les obligations GPAI de la loi européenne sur l'IA suivent désormais un calendrier concret. La barre probante a monté — « nous prenons l'éthique au sérieux » n'est plus une réponse acceptable ; il faut des preuves documentées, par critère, évaluées indépendamment. Et les normes elles-mêmes ont bougé — une grande partie de la documentation de gouvernance existante est périmée.

- Tangram — Où le travail se produit-il, et sous quelles conditions aux frontières ? — Interne : comment nous construisons.
- Origi — Cette action peut-elle se produire, et pouvons-nous prouver ce qui s'est produit ? — Interne : comment nous construisons.
- Helios Grid — Le tissu est-il en santé, à jour et récupérable ? — Interne : comment nous construisons.
- Aegis Defence — Chaque clé et chaque signature survivront-elles à un adversaire quantique ? — Interne : comment nous construisons.
- Aegis Assure — La gouvernance des données d'IA de cette organisation est-elle responsable et défendable ? — Vers l'extérieur : un service que nous livrons.

Le nom est délibéré : Aegis Defence protège les données en mouvement par la cryptographie ; Aegis Assure protège l'organisation en prouvant que ses données ont été gouvernées de façon éthique. Deux boucliers — l'un technique, l'autre probant. Origi et Aegis Assure sont la même philosophie à deux échelles : Origi est un harnais de confiance à l'exécution qui vérifie chaque action d'un système en marche ; Aegis Assure est un cadre d'assurance du cycle de vie qui vérifie chaque étape de la gouvernance des données, périodiquement et au moment de l'accréditation. Une organisation déjà assurée sous Aegis Assure est bien préparée à adopter Origi ; une organisation qui exécute Origi génère en sous-produit une grande partie des preuves qu'Aegis Assure exige. Ils sont conçus pour se composer.

2. Socle réglementaire

Le cadre est délibérément aligné sur des régimes reconnus afin que ses résultats d'accréditation soient défendables à l'externe — et cet alignement suit un paysage qui a matériellement changé. Union européenne : la loi sur l'IA (règlement (UE) 2024/1689) est entrée en vigueur le 1er août 2024 et s'applique par phases — interdictions et obligations de littératie depuis le 2 février 2025 ; gouvernance et obligations des modèles à usage général depuis le 2 août 2025 ; application générale, y compris la plupart des obligations à haut risque, au 2 août 2026 ; systèmes à haut risque intégrés au 2 août 2027.

Canada : la référence antérieure à la LIAD comme « cadre proposé » n'est plus exacte — le projet de loi C-27 est mort au feuillet à la prorogation de janvier 2025, et le Canada n'a actuellement aucune loi fédérale dédiée à l'IA. États-Unis : le décret 14110 a été abrogé en janvier 2025 et remplacé par le décret 14179, réorientant la politique fédérale du risque et des droits vers l'innovation et la compétitivité. Sous ces statuts mouvants demeurent les normes stables qui forment l'ossature technique du cadre : le NIST AI RMF 1.0 et son profil IA générative, ISO/IEC 42001 et 23894, le RGPD et ses homologues — confirmés contre les publications officielles avant tout usage formel.

3. Structure du cadre

Le cadre organise soixante-trois critères uniques en trois parties, selon une seule intuition : les obligations de gouvernance diffèrent par étape du cycle de vie, selon que la donnée entraîne ou opère le modèle, et selon que le contrôle est technique ou organisationnel.

- Section A — Cycle de vie des données — dix étapes, de l'acquisition au retrait, évaluées pour les données d'entraînement et d'inférence — 41 critères.
- Section B — Opération des données — scindée entre opérations d'entraînement et opérations d'inférence, les cinq mêmes codes appliqués différemment à chaque phase — 10 critères.
- Section C — Gouvernance et éthique — critères organisationnels transversaux, propres à aucun projet — 12 critères.

La discipline structurale centrale : les données d'entraînement et d'inférence portent des obligations différentes même sous un même code — l'entraînement soulève la provenance, la portée du consentement, les biais historiques et le droit d'auteur des sources ; l'inférence soulève la validation en temps réel, les entrées adverses et hors distribution. Chaque critère s'exprime sous la forme à deux rôles qui fait la rigueur du cadre : une exigence de preuves que le praticien doit satisfaire, et un guide d'évaluation appliqué pour la juger — la même séparation « preuves puis jugement » qu'Origi impose à l'exécution.

4. Section A — Les critères du cycle de vie

Dix étapes portent quarante et un critères. Chacune énonce sa portée, sa phase applicable et les préoccupations que ses critères évaluent — les codes sont conservés pour la traçabilité vers le classeur d'évaluation.

- Acquisition (AC-01...05) — base légale de la collecte (RGPD art. 6 / PIPEDA / CCPA), provenance et chaîne de possession, biais de collecte, minimisation, propriété intellectuelle.
- Ingestion (IN-01...04) — validation de qualité, normalisation des formats, sécurité à l'ingestion (chiffrement en transit, authentification, journalisation), qualité de l'étiquetage.
- Intégration (IT-01...04) — traçage du lignage de bout en bout, assurance qualité inter-sources, évaluation de l'amplification des biais, gouvernance de l'intégration.
- Classification (CL-01...04) — sensibilité (RPS, catégories spéciales de l'art. 9 RGPD), classification réglementaire, étiquetage entraînement/inférence, alignement des accès.
- Stockage (ST-01...05) — contrôles de sécurité au repos (AES-256, gestion de clés, RBAC/ABAC), rétention, sauvegarde et reprise, journaux d'audit, résilience de l'infrastructure.
- Maintenance (MA-01...05) — actualité des données, nettoyage et correction, rééquilibrage et augmentation, évolution des schémas, intégrité continue.
- Partage et diffusion (SH-01...05, inférence seulement) — gouvernance du partage, protection de la vie privée (anonymisation, confidentialité différentielle), gestion des sous-traitants, limitation d'usage.
- Archivage (AR-01...04) — politique et procédures, sécurité et confidentialité à long terme, documentation et métadonnées, accessibilité durable (migration de formats).
- Retrait (DR-01...05) — suppression sécurisée (effacement cryptographique, multi-emplacements), droit à l'effacement, déclassé des modèles, documentation de disposition.

5. Section B — Les critères d'opération

Cinq critères (OP-01...05) sont évalués deux fois — une fois pour la phase d'entraînement, une fois pour l'inférence — parce que la même préoccupation se comporte différemment dans chacune : surveillance de la qualité et de la dérive, surveillance de la performance, supervision humaine, biais et équité, validation en temps réel. Les critères OP côté inférence sont le point de rencontre le plus direct entre Aegis Assure et Origi : OP-03 (supervision humaine), OP-04 (équité) et OP-05 (détection adverse et hors distribution) décrivent, en termes d'évaluation, exactement les contrôles que le harnais de confiance d'Origi exécute comme application à l'inférence. Une organisation qui exécute Origi produit les preuves de ces critères comme sortie opérationnelle.

6. Section C — Gouvernance et éthique

Douze critères organisationnels s'appliquent à chaque système et à chaque usage des données — ils évaluent la maturité institutionnelle, non un projet isolé.

- Gouvernance organisationnelle (GV-01...03) — structure de gouvernance de l'IA (comité d'éthique, surveillance au niveau du conseil), gestion des risques alignée sur le NIST AI RMF, gestion de la conformité.
- Documentation et transparence (DC-01...03) — documentation technique (fiches de modèles et de jeux de données), explicabilité et interprétabilité (XAI), évaluations d'impact algorithmique.
- Principes éthiques et responsabilité (ET-01...04) — équité et non-discrimination, transparence et responsabilité (recours et contestation), impact sur les droits de la personne, bien-être sociétal.
- Formation et sensibilisation (TR-01...02) — formation et compétence du personnel, culture organisationnelle (mécanismes d'alerte, exemplarité du leadership).

7. Méthodologie d'évaluation

L'intégrité de la méthode repose sur une séparation des devoirs : les praticiens recueillent et documentent les preuves de chaque critère applicable ; les évaluateurs les jugent indépendamment et attribuent les notes. Nul ne produit et ne juge à la fois les preuves d'un même critère — le principe de séparation d'Origine appliqué à l'évaluation.

- Gris — non encore évalué — l'état par défaut.
- Vert — conforme — les contrôles sont efficaces et les preuves soutiennent l'affirmation.
- Ambre — partiel / lacunes mineures — les contrôles existent mais portent des déficiences mineures de conception ou d'exploitation.
- Rouge — non conforme — les contrôles sont absents, inefficaces ou en échec significatif.
- Critique (C) — 40 % — un critère Critique sous le seuil bloque l'accréditation jusqu'à remédiation.
- Élevé (H) — 30 % — exige un plan de remédiation avant l'accréditation.
- Moyen (M) — 20 % — déclenche une feuille de route d'amélioration.
- Faible (L) — 10 % — axe d'amélioration continue.

La règle de blocage est le point décisif : une bonne moyenne ne rachète pas un contrôle Critique en échec — le reflet de la posture « échec fermé » d'Origine. Et la sortie d'un mandat n'est pas une note mais un dossier : par critère, son applicabilité, ses preuves, le raisonnement de l'évaluateur, sa note RAV et son état de remédiation — assemblés en une accréditation de niveau système à la piste d'audit défendable. Dans la langue d'Origine, ce dossier est le dossier d'assurance de la gouvernance des données du système.

8. Mise en œuvre et livraison

Flux du praticien : cadrage -> planification -> collecte des preuves (documentation, entrevues, essais) -> documentation -> identification des écarts -> auto-revue de qualité -> soumission. Flux de l'évaluateur : revue des preuves -> vérification (échantillonnage, essais, entrevues) -> notation RAV -> documentation des constats -> calibrage par les pairs -> rapport (le dossier d'accréditation) -> suivi de la remédiation.

L'accréditation est une position à maintenir, non un certificat à classer. La réévaluation se déclenche par : revue annuelle des systèmes à haut risque déployés ; changement matériel du système (nouvelles sources, changement d'algorithme, extension d'usage) ; changement réglementaire ; incident significatif ou découverte de biais ; passage du pilote à la production. Miovski Group livre le service sous trois formes : une évaluation de préparation (balayage rapide des écarts, RAV seulement), une accréditation complète (le cycle intégral des soixante-trois critères produisant le dossier) et une assurance continue (réévaluation récurrente selon les déclencheurs, intégrable à Origi).

9. Conclusion

Le marché est passé de « le système fonctionne-t-il ? » à l'exigence de prouver que les données qui le sous-tendent ont été gouvernées de façon responsable — et les normes qui définissent une bonne réponse ont suffisamment bougé pour périmé une grande partie de la documentation existante, y compris les références réglementaires antérieures de ce cadre. Cette édition fait les corrections : la LIAD consignée comme morte plutôt qu'en attente, la loi européenne comme calendrier vivant par phases plutôt que texte lointain, la posture américaine comme inversée.

Ce qui ne change pas : la structure et la valeur du cadre — soixante-trois critères sur tout le cycle de vie, la discipline entraînement-contre-inférence, la gouvernance organisationnelle au-dessus des deux, et une méthode à deux rôles, « preuves puis jugement », qui produit un dossier d'accréditation défendable plutôt qu'une opinion. Positionné dans la pile Enkidu, Aegis Assure est le visage extérieur de la même philosophie de confiance qu'Origi impose à l'intérieur des produits de Miovisi Group — le dossier d'assurance, la séparation des devoirs, la primauté de la preuve — offert comme service à toute organisation qui doit désormais prouver, et non plus seulement affirmer, que son IA est bien gouvernée.

La confiance en un système d'IA n'est pas un slogan à proclamer ; c'est une position à argumenter et à prouver. Aegis Assure est la manière dont cette position se construit, critère par critère.