



E N K I D U

— M I O V S K I G R O U P —

É T U D E D E C A S

Trust-Assured Agentic AI

Comment le cadre d'assurance de la confiance et Tangram ont façonné un système multi-agents d'évaluation des capacités pour Environnement et Changement climatique Canada.

Français · Édition condensée

D'après la version 1.0 · 21 juin 2026

Préparé par MIOVSKI GROUP

Classification · Non classifié

L'édition anglaise complète fait foi

À propos de cette édition

Ce document est une édition condensée, en français, de l'étude de cas « Trust-Assured Agentic AI », version 1.0 (21 juin 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 : non classifié.

Résumé

Environnement et Changement climatique Canada (ECCC) devait évaluer la maturité de ses capacités d'affaires et assembler des feuilles de route numériques de direction générale à partir d'un vaste corpus hétérogène de documentation interne — un travail lent, coûteux et subjectif lorsqu'il est fait à la main. Enkidu a construit une preuve de concept (PoC) d'IA agentique multi-agents pour effectuer cette synthèse fidèlement, de façon transparente et répétable, en s'exécutant entièrement sur une infrastructure locale afin de préserver la souveraineté des données.

Cette étude de cas décrit comment deux cadres Enkidu ont été appliqués à ce mandat. Tangram a fourni l'architecture opérationnelle — décomposant le pipeline d'évaluation et de feuille de route en zones bornées et gouvernées, aux transferts explicites. Le cadre d'assurance de la confiance (Origi) a fourni la discipline qui rend les sorties du système défendables — chaque affirmation de confiance liée à une politique, appuyée par un résultat mesurable, justifiée par une chaîne de preuves annotée et traçable au moyen d'un enregistrement de provenance inviolable. La PoC d'ECCC a été, de fait, le premier terrain d'essai de bout en bout des deux cadres.

Le résultat est un système dont la règle centrale — le déterminisme là où il compte, le raisonnement là où il aide — est l'expression directe du principe de pureté des politiques de Tangram et de la séparation des devoirs de l'assurance de la confiance. La notation est une vérité de terrain imposée par le code ; le modèle de langage interprète, extrait les preuves et rédige le récit — mais n'attribue jamais une note finale.

Ne demandez pas qu'on vous fasse confiance — montrez, affirmation par affirmation et étape par étape, exactement pourquoi on le peut.

1. Introduction

Les organisations ont régulièrement besoin de comprendre la maturité de leurs capacités d'affaires pour prioriser l'investissement, conduire la transformation et gérer le risque. L'essentiel des preuves existe déjà à l'interne — transcriptions d'entrevues, documents de processus, post-mortems d'incidents, journaux de changements, constats d'audit — mais les lire et les synthétiser à l'échelle est impraticable pour des humains, et les évaluations menées par des consultants sont coûteuses, subjectives et difficiles à rafraîchir.

ECCC a mandaté Enkidu pour démontrer qu'un système d'IA agentique bien contraint pouvait effectuer cette synthèse à l'échelle tout en restant assez digne de confiance pour éclairer de vraies décisions. Les livrables couvrent une évaluation de maturité des capacités et un ensemble de feuilles de route numériques par direction générale, chacune assemblée à partir de sources ministérielles faisant autorité, avec une traçabilité de citation complète. Parce que ces sorties alimentent des choix d'investissement et de transformation, la barre n'était pas « utile » mais « défendable » : un analyste, un auditeur ou un cadre supérieur doit pouvoir demander, de tout chiffre du rapport, « d'où cela vient-il, et pourquoi devrais-je le croire ? » — et recevoir une réponse complète.

- Ce que montre l'étude — comment Tangram a structuré le pipeline d'évaluation et de feuille de route en zones bornées et gouvernées, aux transferts contractuels.
- Comment le cadre d'assurance de la confiance a transformé « nous croyons ce système digne de confiance » en une position structurée et prouvée — à la livraison comme à l'inférence.
- Comment les deux cadres se sont renforcés mutuellement, et comment la PoC a été étendue en un continuum complet de feuille de route numérique.

2. Les cadres appliqués

Deux cadres Enkidu ont été appliqués au mandat. Ils opèrent à des niveaux différents — Tangram gouverne la forme de l'opération ; l'assurance de la confiance gouverne la fiabilité de ce qui la traverse — et ils sont délibérément complémentaires.

- Tangram — la forme de l'opération — a décomposé le pipeline en zones bornées aux transferts contractuels, politiques pures et chemins d'erreur conçus.
- Assurance de la confiance — la fiabilité du travail — a lié chaque note et affirmation à une politique, une chaîne de preuves et une provenance signée ; vérification zéro-confiance et capacité méritée.

Tangram : toute opération se décompose en zones de service bornées — une zone est une unité de travail à but unique dont la condition de sortie devient la mise d'entrée de la suivante, créant une chaîne de transferts contractuels ; la pureté des politiques garde la gouvernance séparée des opérations ; les erreurs sont des zones de plein droit. L'assurance de la confiance : chaque affirmation est un dossier d'assurance — affirmation, argument, preuves — lié à exactement une politique avec seuil explicite, satisfait seulement quand le résultat mesuré atteint le seuil et que la chaîne de preuves se valide. L'objectif n'est pas la confiance maximale mais la confiance calibrée.

3. La solution ECCC : un système multi-agents

La PoC est un système multi-agents qui ingère un corpus hétérogène de documentation interne, applique des grilles ancrées et déterministes, et produit des notes de criticité, des notes de maturité et un récit structuré des irritants, défis et opportunités, cartographiés sur un modèle de capacités prédéfini. Tout le pipeline s'exécute sur une infrastructure locale pour préserver la confidentialité : une station NVIDIA DGX Spark héberge le modèle de raisonnement (Llama-3.3-Nemotron-Super-49B, servi par un microservice NIM), un magasin vectoriel Chroma, un magasin relationnel léger pour le modèle de capacités et l'historique des exécutions, Arize Phoenix pour l'observabilité et un ensemble de serveurs MCP (Model Context Protocol) — sans aucune sortie réseau à la couche outils.

La règle centrale : le déterminisme là où il compte, le raisonnement là où il aide. Formules de notation, grilles, pondérations et modèle de capacités sont une vérité de terrain imposée par le code ; le modèle de langage interprète, extrait et rédige — jamais d'arithmétique, jamais de note finale. Le système ne produit jamais « juste » un chiffre : il produit un chiffre plus sa dérivation complète et rejouable.

L'orchestration suit un patron superviseur/spécialistes plutôt qu'un essaim libre : chaque agent est un nœud de flux au rôle étroit, au contrat de sortie explicite et aux outils déclarés — et l'agent qui extrait les preuves n'est jamais celui qui note, ni celui qui rédige.

- Superviseur — planifie l'exécution, sélectionne les capacités à analyser, répartit le travail et impose critères d'achèvement et plafonds de coût.
- Récupération — extrait de Chroma les segments documentaires les plus pertinents, par similarité vectorielle et filtres de métadonnées.
- Extraction de preuves — lit les segments et en tire des éléments structurés — irritants, défis, opportunités — chacun avec citation de source.
- Notation — applique la grille ancrée aux preuves et appelle le MCP de notation pour calculer la valeur pondérée finale, en code.
- Critique — revoit indépendamment la notation contre les preuves et la grille, signale les incohérences et peut forcer une renotation.
- Agrégateur — consolide les résultats par capacité en vue organisationnelle et dégage les motifs systémiques.
- Récit — produit le récit lisible du rapport, sans rien écrire qui ne soit fondé sur les notes structurées et les preuves citées.

4. Tangram en pratique : le continuum de feuille de route

Le pipeline ECCC s'applique proprement sur Tangram. Le flux de bout en bout — des documents bruts de la direction générale à la feuille de route numérique complétée — est un seul continuum, et chaque étape analytique est une zone à but unique et aux conditions de frontière explicites. Les invites qui pilotent le système deviennent visibles comme définitions de zones : rôle, sources autorisées (contrainte dure), flux de travail par phases obligatoire, exigences de citation et porte de couverture — en termes Tangram : but de zone, mises d'entrée, conops et conditions de sortie.

- Analyse du plan d'affaires — transformer le plan d'affaires de la direction générale en constats stratégiques, initiatives classées et matrice d'actions — sortie : un classeur validé qui passe la porte de couverture.
- Objectifs et moteurs — dériver l'ancrage stratégique : objectifs, moteurs et parrains — chaque cellule traçable au classeur d'analyse.
- État actuel — établir la référence telle quelle des capacités, applications, données et irritants — notée contre les dimensions de maturité.
- État cible — dériver la vision à atteindre du plan ministériel, filtrée pour la direction générale — source de toute initiative ultérieure.
- Initiatives — lister les initiatives discrètes menant de l'état actuel à l'état cible — portefeuille avec responsables, livrables et mesures, tous cités.
- Recommandations technologiques — produire la réponse technologique, ancrée aux objectifs et aux initiatives.

La pureté des politiques apparaît directement dans les contraintes dures du pipeline : « n'utilise aucune connaissance extérieure ; si les sources sont insuffisantes, dis-le ; si elles divergent, expose le conflit » — une politique pure, au verdict déterministe. Et les erreurs sont des zones de plein droit : un échec de porte de couverture ne laisse rien tomber en silence — il produit un rapport de couverture qui liste chaque lacune ; une discordance de nom de direction générale arrête l'exécution et demande confirmation. Si votre seul traitement d'erreur est « contactez un superviseur », vous avez une zone non conçue — le pipeline ECCC conçoit ses échecs à l'avance.

5. L'assurance de la confiance en pratique

Là où Tangram façonne le pipeline, le cadre d'assurance de la confiance rend ses sorties défendables. La PoC a été le premier système à exercer le cadre de bout en bout, et la correspondance est concrète : les neuf composantes de confiance, le modèle de provenance et le harnais de confiance à l'inférence correspondent chacun à un dispositif précis du système déployé.

- Compétence et fiabilité — grilles ancrées et déterministes, modèle de capacités fixe ; performance validée contre un jeu d'évaluation étalon-or.
- Transparence et explicabilité — raisonnement structuré « preuves puis jugement » ; chaque note remonte à des preuves citées et à une bande de grille appliquée.
- Confiance calibrée — la fausse assurance est gardée par un agent critique indépendant et des évaluateurs d'ancrage ; les éléments faiblement étayés sont écartés, non affirmés.
- Prévisibilité et cohérence — version de modèle fixe, invites versionnées et formules déterministes rendent les exécutions reproductibles et comparables dans le temps.
- Responsabilité et recours — piste d'audit complète des documents, grilles, appels d'outils et notes ; point de contrôle humain avant toute diffusion du rapport.
- Équité et gestion des biais — notation de maturité désagrégée par direction et dimension, exposant les sous-groupes faibles qu'une moyenne masquerait.
- Sécurité et robustesse — assainissement des documents, rails anti-injection, listes d'outils autorisés par agent et aucune sortie réseau à la couche outils.
- Alignement sur l'intention — l'application du périmètre garde les agents dans le mandat d'évaluation ; le modèle n'attribue jamais de note finale.
- Agentivité et dépendance humaines — la PoC est explicitement une aide à la décision, non un décideur autonome ; le rapport final est revu par un analyste humain.

La chaîne de preuves inviolable se réalise par des contrats de sortie structurés, l'imposition des citations et l'observabilité intégrale : chaque message inter-agents suit un schéma validé ; chaque élément de preuve et chaque note portent une citation résolvable jusqu'au document et au segment ; les sorties sans citation sont rejetées. La différence sur laquelle le cadre insiste : non pas « un chiffre que quelqu'un a tapé », mais « un chiffre qu'un processus nommé et vérifiable a produit ».

- Pré-vol (entrée) — l'assainissement retire le contenu actif ; les rails d'entrée détectent les motifs d'injection et rejettent les demandes hors périmètre avant tout contexte d'agent.
- En vol (à chaque étape) — listes d'outils autorisés par agent (moindre privilège) ; MCP de fichiers borné aux répertoires désignés ; budgets d'outils par exécution contre l'emballement.
- Post-vol (sortie) — validation de schéma, imposition des citations, contrôles d'ancrage et filtrage des renseignements personnels avant toute écriture au rapport final.

La capacité méritée apparaît dans le modèle de permissions : la plupart des outils sont en lecture seule ; seuls le constructeur de rapport et un rédacteur de fichiers borné mutent — l'accès en écriture est la capacité la plus étroitement accordée du système. Et la séparation des devoirs — nul composant ne juge et n'exécute à la fois — est portée par le patron superviseur/spécialistes lui-même.

6. Étendre la preuve de concept

La PoC établie, le mandat l'a étendue d'une seule étape d'évaluation à l'ensemble du continuum de feuille de route numérique. Chaque extension a été ajoutée de la même manière : une nouvelle zone aux mises d'entrée explicites, une politique pure de sources et de citations, un chemin d'erreur de porte de couverture conçu, et la même discipline de provenance. La nouvelle fonctionnalité n'a rien relâché — parmi les nouvelles entrées : une évaluation de maturité notée sur vingt-trois dimensions de capacités et une analyse d'irritants notée de façon déterministe.

7. Résultats et conclusion

Le mandat ECCC a livré un système multi-agents fonctionnel, sur site, qui évalue la maturité des capacités d'affaires et assemble des feuilles de route numériques de direction générale à partir de sources faisant autorité — fidèlement, de façon transparente et répétable. Tout aussi important : il a prouvé les deux cadres Enkidu dans un seul déploiement réel.

Tangram a donné au mandat une architecture opérationnelle qu'un architecte d'entreprise lit d'un coup d'œil : un continuum de zones bornées, des transferts contractuels, des politiques pures et des chemins d'erreur conçus. Le cadre d'assurance de la confiance a donné au même mandat une position de confiance défendable : neuf composantes réalisées chacune par un mécanisme concret, une chaîne de preuves inviolable derrière chaque note, et un harnais zéro-confiance qui vérifie chaque étape à l'inférence. Les deux se rejoignent dans la règle centrale du système — le déterminisme là où il compte, le raisonnement là où il aide — à la fois frontière de politique Tangram et séparation des devoirs de l'assurance de la confiance.

Le résultat est l'objectif déclaré du cadre devenu réel : non pas la confiance maximale, mais la confiance calibrée — une dépendance proportionnée à la fiabilité démontrée — appuyée par un dossier vérifiable qu'un analyste, un auditeur ou un cadre supérieur d'ECCC peut interroger. La PoC est achevée ; les cadres qui l'ont façonnée sont désormais éprouvés, et le patron qu'elle établit est réutilisable pour le prochain déploiement gouverné augmenté par l'IA.

La confiance calibrée, méritée affirmation par affirmation et étape par étape — et une architecture opérationnelle assez lisible pour le prouver.