La maturité IA des actifs

March 10, 2025 • 22 min read

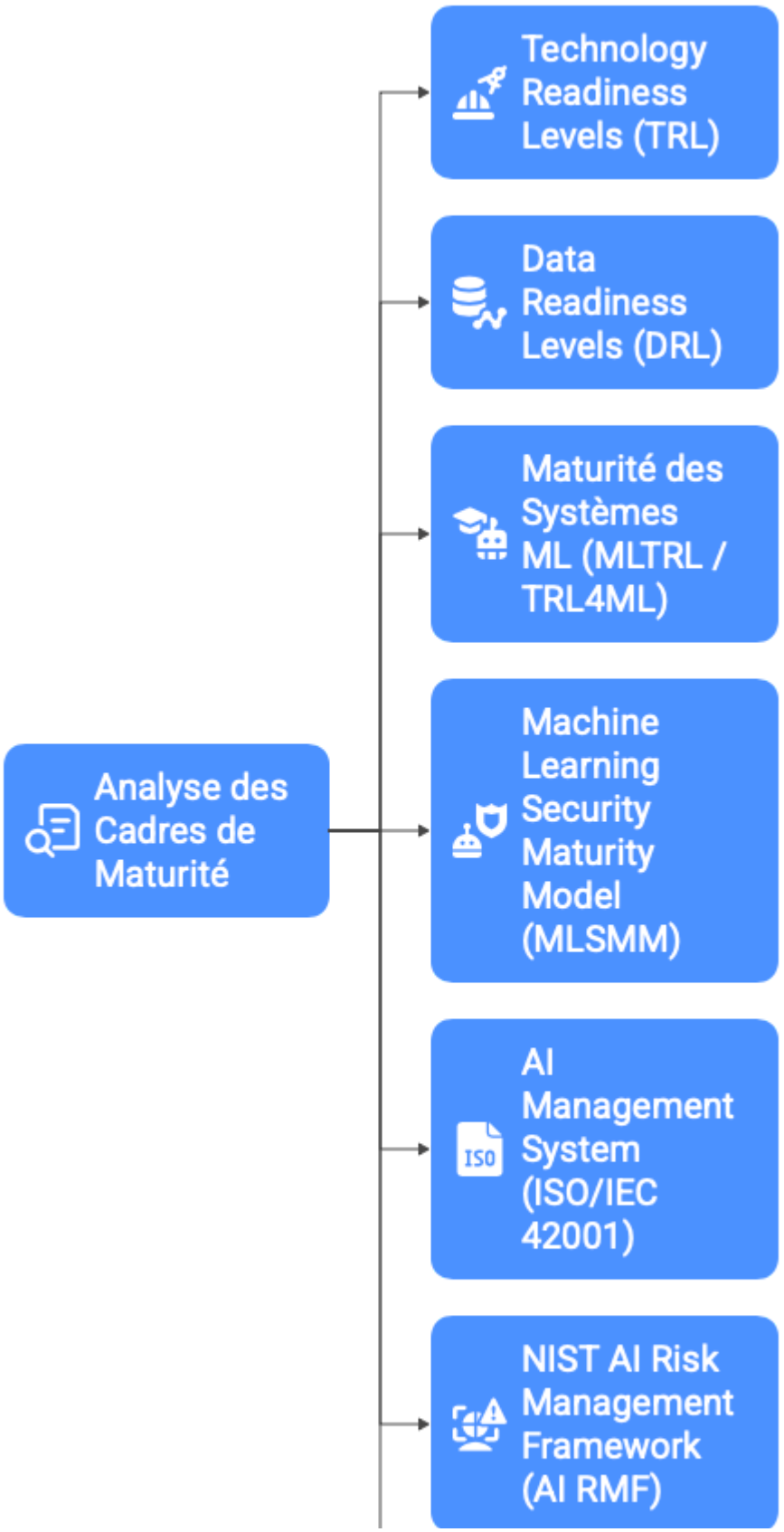
TRL IA Maturité

Maturité des assets IA

Ce document propose une analyse approfondie des principaux cadres de maturité des assets d'IA. Avec des exemples concrets pour piloter la maturité des données, des modèles, des prompts, des pipelines, des agents et des systèmes d'IA. L'objectif n'est pas d'ajouter un nouveau framework, mais de s'appuyer sur les référentiels existants, qui sont déjà nombreux. Cette liste n'est d'ailleurs pas exhaustive :

- Technology Readiness Levels (TRL trl nasa)
- Data Readiness Levels (DRL arxiv-Neil D. Lawrence-2017)
- maturité des systèmes ML (MLTRL / TRL4ML Arxiv-Alexander Lavin al.-2022)
- Machine Learning Security Maturity Model (MLSMM) Arxiv-Felix Viktor Jedrzejewski al.-2023)
- AI Management System (ISO/IEC 42001 ISO)
- NIST AI Risk Management Framework (AI RMF)(NIST)
- Approches émergentes d'**AI Security Posture Management (AISPM)**

Cadres de Maturité pour les Assets d'IA



> *Oui, j'ajoute encore 3 niveaux de plus... À ce stade, notre collection de "RL" commence sérieusement à ressembler à un Pokédex de cadre maturité ... disons que nous ajoutons des évolutions de Pokémons.*

Bien que ce document s'appuie sur des cadres déjà établis (Technology Readiness Levels - TRL, Data Readiness Levels – DRL, Machine Learning Technology Readiness Levels – MLTRL, etc.), il convient de préciser que les trois dimensions suivantes ne sont pas simplement " de nouveaux " cadres inventés mais plutôt des dérivés d'existants :

- **SecRL (Security Readiness Levels)** : le projet européen MultiRATE décrit explicitement une échelle *Security Readiness Level (Sec RL)* à 9 niveaux, alignée sur les autres échelles de readiness (TRL, IRL, CRL...) afin d'évaluer la maturité de la **sécurité** d'une technologie ou d'un actif. En parallèle, les travaux sur les " AI Security Maturity Models " indiquent que la dimension " sécurité IA " est bien identifiée comme un axe de maturité indépendant (contrôles de sécurité, monitoring, robustesse adversaire...). (m4d.iti.gr) Dans ce document, SecRL est proposé comme adaptation **au niveau des assets IA**.
- **GovRL (Governance Readiness Levels)**: bien que le terme exact "GovRL" ne soit pas largement utilisé dans la littérature (il est probablement inventé ici), l'idée est largement soutenue par plusieurs travaux : par exemple, le modèle AI Governance Maturity Model (IEEE-USA) exploite une fiche de maturité pour la gouvernance de l'IA, s'appuyant sur le NIST AI Risk Management Framework (AI RMF). (IEEE-USA) Des modèles commerciaux et de marché décrivent également des "AI Governance Maturity Models" couvrant des niveaux d'adoption, de documentation, de surveillance et de gouvernance de l'IA (zendata.dev). Ici, GovRL est proposé comme version "asset-centrée" de cette gouvernance IA : on mesure non seulement

"l'organisation" de la gouvernance IA, mais aussi la maturité de la gouvernance **pour chaque actif IA**.

- **OpsRL (Operations Readiness Levels)** : ici aussi, l'expression " OpsRL " n'est pas couramment utilisée ; la notion d'"Operational Readiness" (préparation opérationnelle — capacité d'une organisation ou d'un système à passer en exploitation) est bien documentée. (Wikipedia) Dans notre cadre, OpsRL désigne le niveau de maturité opérationnelle d'un *asset* IA (pipeline, modèle, infrastructure) : du prototype "expérimental" à un service pleinement opéré, monitoré, automatisé et scalable.

Ainsi, SecRL, GovRL et OpsRL s'inscrivent dans un continuum de readiness/maturité, en complément des axes technologiques (TRL/MLTRL), données (DRL) et opérationnels (MLOps/ops-readiness). Leur ajout permet de renforcer la couverture du spectre : non seulement " Quelle technologie est prête ? ", mais aussi " Cette technologie est-elle sécurisée ? Et bien gouvernée ? " ...

Beaucoup d'assets IA "récents", par exemple des modèles génératifs, des agents autonomes ou des composants IA multi-domaines, reposent sur des technologies à **forte généralité**. Or, selon AI Watch, " plus une techno d'IA est spécialisée, plus elle grimpe facilement les marches du TRL... mais dès qu'elle devient un peu trop générale, les niveaux élevés restent aussi inatteignables qu'un boss final de niveau 99 ". (AI Watch) ... même si ces assets sont déjà exposés à des utilisateurs finaux, il est raisonnable d'estimer qu'ils se situent dans une zone TRL **3 à 7**, plutôt qu'à TRL 8 ou 9, en raison de la complexité, du besoin de robustesse multitâche et des conditions opérationnelles encore peu éprouvées.

Pourquoi mesurer la maturité des assets IA ?

Plusieurs dynamiques structurent désormais tout projet IA : la course des use cases, la maturité réelle des assets et la dimension humaine de la gouvernance. Elles expliquent pourquoi certains projets décollent ... et pourquoi tant d'autres restent bloqués sur le tarmac.

Les projets avancent plus vite que les socles

Les organisations combinent déjà des modèles de scoring, moteurs de recommandation, optimisation opérationnelle, des modèles génératifs, chatbots, RAG, agents ou encore des projets exploratoires au sein d'équipes métier (souvent en dehors des circuits officiels).

Mais de nombreux projets restent **bloqués en POC**, faute de données prêtes, d'industrialisation MLOps ou d'un cadrage des risques suffisant (arXiv). Les incidents "IA" (fuites de données, réponses inappropriées, biais) présentent souvent un terreau similaire : données peu maîtrisées, modèles non monitorés, responsabilités diffuses (Hyperproof). Pour finir, les cadres réglementaires (AI Act, exigences sectorielles) et normatifs (ISO 42001, NIST AI RMF) demandent une **traçabilité** et une **gouvernance** accrues des systèmes d'IA.(ISO)

Quand bien même les TRL donnent une vue sur la **maturité du système**, ils ne disent pas à quel point les **données** sont maîtrisées, comment les **modèles** ont été conçus, testés et documentés, quel est le niveau de **sécurité de l'IA**, qui **porte le risque** au quotidien, dans quel état sont les **opérations** (pipeline, infra, monitoring).

Valeur pour la recherche, la tech, le business, le marketing

DRL et MLTRL ont été conçus pour structurer la transformation de résultats de recherche en systèmes utilisables.(arxiv-Neil D. Lawrence-2017) Une grille de maturité des assets IA permet de prioriser les travaux sur les **données** (élévation du DRL) autant que sur les modèles, d'éviter de produire des démonstrateurs "non industrialisables par construction" et d'identifier les **assets IA stratégiques** (datasets propriétaires, modèles robustes) qui méritent un investissement renforcé.

Pour ce qui est du Data / ML / Engineering / Ops, les cadres DRL; MRL et OpsRL permettent de **prioriser les chantiers d'industrialisation** (feature store, pipelines, monitoring, observabilité)(digital.nemko.com). SecRL fournit un langage pour intégrer les exigences de sécurité de l'IA (tests adversariaux, posture de sécurité, AISPM) dans les roadmaps techniques. Et GovRL permet d'aligner les efforts techniques avec la trajectoire de conformité (ISO 42001, NIST AI RMF, AI Act).(ISO)

Pour un COMEX ou une direction métier, le TRL répond à la question : "Cette solution est-elle prête à être testée, déployée ou généralisée ?". Quant à la maturité des assets IA, elle répond à : "Sur quoi repose-t-elle ? Quel est le socle ? Peut-on le réutiliser ailleurs ? Est-il maîtrisé ?"

Et pour finir, la capacité à démontrer l'origine des données, prouver l'existence de contrôles, fournir une AI-BOM (encore très - **TRES** - peu utilisée) / fiches d'assets IA devient une **proposition de valeur** dans les relations B2B/B2G, et un élément de crédibilité sur le terrain de "l'IA responsable".

Dimension humaine et politique d'entreprise

La maturité des assets IA n'est pas qu'un sujet de référentiel mais une question de **pouvoir** (qui décide ?), de **responsabilité** (qui signe ?), et de **capacité à dire non** (ou à dire "pas encore").

> *“La maturité des assets IA, c'est pas qu'une affaire de référentiel : c'est qui décide, qui signe… et qui ose dire non.” En gros, tant qu'on n'a pas clarifié ça, on ne gère pas l'IA : on se refile la patate chaude et qu'à la fin tout le monde jure que ce n'est pas sa main qui fume.*

Il est illusoire de vouloir tout centraliser dans un rôle unique ("Model Owner" héroïque). La responsabilité doit être **partagée**, explicite et reliée aux instances de décision existantes (comités risques, architecture, métiers).

Panorama des cadres existants (veille)

> *Les cadres "Readiness Level", c'est un peu comme un dîner de famille à la campagne : il y a plus de de bétail que de convives et l'odeur pique le nez au début, mais on s'y habitue.*

TRL – Technology Readiness Levels

Standard pour la maturité technologique des systèmes (1–9), utilisé dans l'aérospatial, la défense, les programmes européens, etc.(nasa). On peut le découper en 3 grandes parties:

- recherche et preuve de concept (TRL 1 à 3);

- prototypes et validations (TRL 4 à 6);
- démonstration, qualification, exploitation (TRL 7 à 9).

DRL – Data Readiness Levels

Proposé par Neil Lawrence (2017), DRL distingue trois "*bands*" (C/B/A) pour décrire l'accessibilité des données (de la simple hypothèse à la donnée chargée), la qualité / validité des données (nettoyage, exploration, représentativité) et l'utilité des données pour une tâche spécifique (format, contexte, conformité). Chaque bande peut être subdivisée (ex. C4→C1, B3→B1, A3→A1) afin de donner davantage de granularité. (arxiv-Neil D. Lawrence-2017)

Cette grille permet de poser une langue commune : " où en sont mes données ? ", d'évaluer les efforts restants avant modélisation ou exploitation, et de mieux planifier les ressources (ingénierie de données, nettoyage, conformité, etc.). Bien que le cadre soit générique, des travaux de la communauté ont commencé à proposer des versions plus opérationnelles (checklists, critères par niveau) dans certains secteurs ou contextes (ex. documentation NLP-data-readiness) ; toutefois, un référentiel universel "par secteur" validé reste à consolider, donc utiliser ces déclinaisons avec prudence.

Des travaux récents affinent ces bands en critères opérationnels, par secteur. (pure.tue.nl)

MLTRL – Machine Learning Technology Readiness Levels

MLTRL transpose les TRL au cycle de vie des systèmes ML.(Arxiv-Alexander Lavin al.-2022)

Pour comprendre on peut *mapper* les MLTRL sur les TRL → MLTRL:

- TRL 0 - 2 → MLTRL 0–2 : Recherche, Idée → principes → premières expériences, souvent sur données simulées ou partielle.
- TRL 3 - 4 → MLTRL 3–4 : Prototype & Proof-of-Concept, Code prototype, premières intégrations, PoC sur vraies données.

- TRL 5 → MLTRL 5 : Capability, Le modèle devient une capacité ML exploitable, transmise à l'ingénierie.
- TRL 6–7 → MLTRL 6–7 : Développement produit + Intégration, Productisation, API propres, pipelines réels, tests, CI/CD, qualité.
- TRL 8 → MLTRL 8 : Flight-ready, Tests avancés : A/B, shadow, canary, data-drift, robustness.
- TRL 9 → MLTRL 9 : Deployment + Monitoring continu, Déploiement, observabilité ML, dérive des données, boucle d'amélioration.

MLSMM – Machine Learning Security Maturity Model

Le *Machine Learning Security Maturity Model* (MLSMM) est un modèle de maturité proposé pour évaluer et améliorer les pratiques de sécurité dans le développement de systèmes basés sur l'apprentissage automatique. C'est un cadre "léger" et agnostique au domaine, conçu pour combler le manque de modèles spécifiques à la sécurité ML par rapport aux approches traditionnelles en développement logiciel.

C'est un prototype conceptuel, non encore validé empiriquement à grande échelle.

ISO/IEC 42001 – AI Management System (AIMS)

C'est un norme internationale certifiable dédiée à la gestion responsable de l'IA. Elle définit les exigences d'un système de management de l'intelligence artificielle. Elle impose à toute organisation (entreprise, administration, association) qui développe, fournit ou utilise des systèmes d'IA de mettre en place un cadre complet couvrant : la cartographie des risques IA tout au long du cycle de vie, l'évaluation d'impact, la gouvernance, la traçabilité des données et modèles, la mesure de la performance éthique et technique, la gestion des incidents et l'amélioration continue. Conçue pour être compatible avec le NIST AI RMF et l'EU AI Act, elle devient rapidement la référence pour les certifications " IA responsable " et est déjà exigée dans certains appels d'offres publics et contrats B2G/B2B. (ISO)

NIST AI RMF

Ce cadre est conçu comme un guide volontaire et non contraignant (contrairement à l'AI Act), il fournit une méthodologie structurée et pragmatique pour identifier, évaluer, prioriser et gérer les risques liés aux systèmes d'IA tout au long de leur cycle de vie.

Organisé autour de quatre fonctions principales : Govern (gouvernance), Map (cartographier le contexte et les risques), Measure (mesurer et évaluer), Manage (gérer et atténuer). Il met particulièrement l'accent sur les risques émergents comme les biais, la perte de confidentialité, la sécurité adversariale, les hallucinations ou les impacts sociétaux. Largement adopté par les entreprises américaines et internationales.

Il sert de socle de conformité pour de nombreuses réglementations et est explicitement reconnu comme compatible avec l'ISO/IEC 42001 et l'EU AI Act. En pratique, il est devenu le " langage commun " de la gestion du risque IA dans le monde anglophone et au-delà.(NIST)

DataOps / MLOps / DevOps / SecOps

Les analyses récentes convergent : beaucoup de modèles restent à l'état de prototype faute de pipelines robustes.(arXiv). Le MLOps implique des coûts non négligeables (plateforme maison ou assemblage de briques), amplifiés par le coût des GPU, la nécessité de gérer plusieurs générations de modèles, les exigences d'auditabilité.

Focus sur les *assets IA* et la réalité d'un inventaire

On peut considérer un *asset IA* tout composant identifiable, doté d'une valeur potentielle de réutilisation, porteur de risques spécifiques.

Typiquement :

- **données** : sources, datasets, features, bases RAG ;
- **modèles** : internes, open source, tiers, fine-tunés ;
- **prompts / agents** : prompts systèmes, workflows, agents ;
- **pipelines & services** : entraînement, inférence, orchestration ;

- **artefacts de gouvernance** : AI-BOM, fiches modèles, registres de risques IA.

Mettre en place un inventaire exhaustif est rarement réaliste à court terme la dispersion (notebooks, repos Git, outils SaaS, scripts locaux), la diversité des pratiques (shadow AI dans différentes équipes) elt les efforts de mise à jour continu sont difficile à financer sur la durée. Même pour le logiciel "classique", la mise à jour d'un SBOM complet reste un challenge.(digital.nemko.com)

Ces difficultés ne veulent pas dire qu'il ne faut rien faire, on peut imaginer un inventaire ciblé et progressif en ciblant d'abord les systèmes à enjeux (IA à impact client / citoyen, fort impact financier , haut risque au sens AI Act). Puis en travaillant par vagues. Avoir un schéma de données (ype d'asset, owner, liens de dépendance, exposition, maturité synthétique). Finalement essayer d'automatiser.

Maturité des assets IA et articulation avec le TRL du système

Pour construire cet AI Asset RL (AIA-RL), on associe 5 niveaux (où 1 = totalement informel, 5 = industriel, certifiable, réutilisable à l'échelle du groupe) AI aux cadres existants. L'AIA-RL global d'un asset ou d'un système est toujours l'**AIA-RL_min** = le score le plus bas parmi les cinq dimensions (DRL, MRL, SecRL, GovRL, OpsRL).

Comment chaque grand cadre existant est condensé dans chaque dimension de l'AIA-RL

DRL : maturité des données (source : Data Readiness Levels – Neil Lawrence 2017 + déclinaisons opérationnelles)

- AIA-RL 1 : bande C (hypothétique ou inaccessible), les données existent " dans la tête " de quelqu'un ou dans un fichier personnel non partagé.
- AIA-RL 2 : bande C / début B (données accessibles mais brutes), l'accès contractuel est validé, la source connue, le propriétaire désigné, mais pas de pipeline, pas de nettoyage systématique.
- AIA-RL 3 : bande B (données utilisables), le pipeline de préparation est versionné, il y a quelques indicateurs de qualité mesurés et historisés, le schéma documenté.

- AIA-RL 4 : bande A (données prêtes pour l'industrialisation), le feature store ou data lakehouse existe, il y a des tests automatisés de qualité et de conformité, il y a des possibilité de réutilisation cross-projet.
- AIA-RL 5 : bande A avancée + certification, les données sont auditables, tout est certifié RGPD/AI Act, versionnées comme du code et réutilisables immédiatement par n'importe quelle équipe du groupe.

MRL : maturité du ou des modèles (Arxiv-Alexander Lavin al.-2022, niveaux 0 à 9 condensés)

- AIA-RL 1 : MLTRL 0-1, l'idée ou un notebook unique non reproductible existe
- AIA-RL 2 : MLTRL 2-3, le code est versionné, l'entraînement scripté, les métriques enregistrées, mais c'est encore du " research code ".
- AIA-RL 3 : MLTRL 4-5, le model card est complet, les tests unitaires existent, la validation est effectuée, l'asset est remis officiellement à l'ingénierie.
- AIA-RL 4 : MLTRL 6-7, il existe un registre de modèles, une gestion des versions sémantiques, des tests de non-régression automatisés et une API propre.
- AIA-RL 5 : MLTRL 8-9, le modèle est publié dans un catalogue interne ou public, les benchmarks comparatifs sont publiés, le monitoring de performance est en production, la boucle d'amélioration continue est en place.

SecRL : maturité sécurité IA

- AIA-RL 1, aucun contrôle spécifique IA : on traite le modèle comme un logiciel classique.
- AIA-RL 2, tests adversariaux manuels sur quelques exemples, scan basique de dépendances PyPI/HuggingFace.
- AIA-RL 3, tests adversariaux automatisés dans le CI/CD, rate limiting, guardrails basiques, scan supply-chain systématique.
- AIA-RL 4, red teaming formalisé, monitoring en production des attaques (prompt injection, jailbreak, data poisoning), politique de divulgation des vulnérabilités.

- AIA-RL 5, AISPM complet, certification tierce de robustesse adversariale, bug bounty dédié aux modèles, conformité ISO 42001 annexe A.8.

GovRL : maturité gouvernance & conformité (sources : ISO/IEC 42001 + NIST AI RMF fonctions Govern/Measure/Map/Manage)

- AIA-RL 1, personne n'est formellement responsable, aucune fiche.
- AIA-RL 2, un owner métier est désigné, fiche modèle partiellement remplie.
- AIA-RL 3, on dispose de fiche modèle + fiche données + registre des risques IA + revue formelle à trois voies (métier/tech/risk) avant chaque déploiement.
- AIA-RL 4, un AI-BOM est générée automatiquement, workflow d'approbation intégré dans les outils (Jira, ServiceNow), il y a un reporting automatisé vers le comité risques.
- AIA-RL 5, la gouvernance est intégrée au comité risques entreprise, audit externe annuel, reporting réglementaire (AI Act fundamental rights impact assessment) automatisé.

OpsRL : maturité opérationnelle (sources : MLOps Maturity Model Google/CMU + pratiques DataOps/SecOps)

- AIA-RL 1, déploiement manuel sur une machine unique.
- AIA-RL 2, script de déploiement versionné, logs accessibles.
- AIA-RL 3, CI/CD complet, monitoring basique (latence, taux d'erreur), rollback manuel.
- AIA-RL 4, canary / shadow deployment, monitoring de dérive conceptuelle et données, alertes automatiques, feature flags, coût par inférence tracé.
- AIA-RL 5, plateforme MLOps partagée groupe, SLA contractualisés internes, autoscaling GPU, gestion multi-génération de modèles, observabilité full-stack (traces OpenTelemetry).

... En associant à l'échelle TRL ...

- AIA-RL_min = 1 : TRL maximum crédible = 3 (expérimentation interne uniquement)
- AIA-RL_min = 2 : TRL maximum crédible = 5 (pilote très encadré, jamais sur données sensibles)

- AIA-RL_min = 3 : TRL maximum crédible = 7 (production possible, mais périmètre limité et surveillance renforcée)
- AIA-RL_min = 4 : TRL maximum crédible = 8 (production à grande échelle acceptable)
- AIA-RL_min = 5 : TRL 9 possible (système pleinement opérationnel, certifiable, réutilisable partout)

> *AIA-RL et TRL : plus tu montes, plus tu te rapproches du côté lumineux de la prod. "Mapper ou ne pas mapper... fais-le, ou ne le fais pas. Il n'y a pas d'essai." (Maitre AIA ,AIA-RL VI : Le Retour du TRL-di)*

En appliquant systématiquement ce mapping précis et cette règle de compatibilité AIA-RL_min → TRL max, plus aucun débat stérile " on est TRL 7 mais ça explose en production " n'a lieu d'être.
On voit immédiatement quel référentiel existant (DRL, MLTRL, ISO 42001, NIST AI RMF, MLSMM, etc.) est en cause, quel est le chantier prioritaire, et surtout quel niveau de TRL on peut raisonnablement viser à horizon 6, 12 ou 24 mois.

Contraintes, difficultés et points de vigilance

Beaucoup d'organisation ont déjà leur modèle de maturité data, leur grille sécurité, leur référentiel architecture, leur TRL maison. La grille AIA-TRL cadre simplement ce qui est nécessaire pour l'IA et ajoute une contrainte sur l'échelle TRL.

Coûts et efforts : fourchettes réalistes

Les données publiques et retours de terrain montrent que la mise en place d'une AI governance alignée AI Act + ISO 42001 sur un grand groupe sur la première année est souvent **de l'ordre du million d'euros** (1–3 M€) si l'on inclut le temps interne (juridique, risk, data, IT), l' accompagnement externe et l'outillage (inventaires, monitoring, sécurité)

En régime de croisière plusieurs centaines de k€ par an (0,5–1,5 M€) sont nécessaire selon le périmètre et le degré d'automatisation. Ainsi, pour des acteurs fortement exposés (banque, santé, grand public), on constate qu'il est nécessaire de disposer d'un noyau de 3–5 ETP internes dédiés à la

gouvernance IA (coordination, juridique, risk, data) et un halo de 10–15 ETP équivalents en incluant les contributions des métiers, de la sécurité, de l'IT, et des prestataires formation / conseil.

Par ailleurs, les coûts MLOps ne sont pas négligeable : le développement et exploitation de plateformes MLOps sur mesure nécessite des investissements initiaux estimés dans la littérature entre ~1 et 20 M$ avant surcoûts récents (GPU, sécurité IA) et en pratique, les retours récents suggèrent d'anticiper un surcoût de 30–50 % (à cause de la montée en puissance des LLM,des pénuries / prix des GPU,d es exigences d'auditabilité).

En conclusion, pour viser GovRL / SecRL / OpsRL à 4–5 sur quelques systèmes IA critiques, il faut assumer un ticket d'entrée à 7 chiffres pour un grand groupe. Pour viser **2–3** sur un périmètre ciblé, une organisation moyenne peut rester dans des enveloppes **nettement inférieures**, en s'appuyant sur des solutions SaaS, des pratiques organisationnelles, des dispositifs "lean".

Ordres de grandeur économiques et scénarios

Pour rendre le cadre exploitable, il est utile de proposer des **scénarios de coût**.

Scénario "Essentiel" (organisation moyenne, ressources limitées)

Objectif : porter quelques systèmes IA clés à :

- **DRL / MRL / SecRL / GovRL / OpsRL ~ 2–3**,
- sur un horizon 18–36 mois.

Ordre de grandeur :

- **Budget annuel** : 150–400 k€ environ, selon :
  - usage de solutions SaaS vs on-prem,
  - recours au conseil,
  - ampleur des formations.
- **Ressources** :

- 0,5–1 ETP de coordination IA/gouvernance,
- contributions ponctuelles des équipes existantes.

Scénario "Cœur" (ETI avancée ou grande BU)

Objectif : structurer la maturité des assets IA pour un domaine (par ex. risque, distribution) :

- plusieurs dizaines d'assets IA (modèles, datasets, pipelines) ;
- cible : **AIA-RL_min 3** sur les systèmes IA les plus critiques.

Ordre de grandeur :

- **Budget annuel** : 400 k€ – 1,2 M€ (gouvernance IA, MLOps de base, outils de découverte / inventaire, AISPM léger).
- **Ressources** :
  - 2–3 ETP dédiés au pilotage IA (gouvernance, data, MLOps),
  - 5–10 ETP équivalents en contribution dans les équipes.

Scénario "Étendu" (groupe multi-BU / secteur régulé à forte exposition)

Objectif : appliquer la grille à plusieurs centaines d'assets IA, à des systèmes IA à haut risque, multi-juridictionnels et pour viser **AIA-RL 3–4** sur les systèmes critiques.

Ordre de grandeur :

- **Budget annuel** : 1–3 M€ (parfois plus), incluant :
  - AIMS ISO 42001 étendu,
  - plateformes MLOps / AISPM,
  - tooling AI-BOM / inventaires,
  - programmes de formation et de conduite du changement.
- **Ressources** :
  - 3–5 ETP internes cœur IA/gouvernance,
  - 10–15 ETP équivalents en contributions métiers / IT / risk / juridique.

Trajectoire d'adoption graduelle

Étape 1 – S'adosser aux TRL existants

- Identifier comment les TRL sont utilisés aujourd'hui (formels ou informels).
- Décider que **tout système IA** devra être positionné sur :
  - une **échelle TRL**,
  - une **grille de maturité des assets IA** (AIA-RL) au moins sur les systèmes à enjeu.

Étape 2 – Expérimenter la grille AIA-RL sur un périmètre pilote

- Sélectionner 5–10 systèmes IA représentatifs.
- Évaluer DRL, MRL, SecRL, GovRL, OpsRL (évaluation qualitative guidée).
- Produire :
  - une matrice TRL × AIA-RL pour ces cas,
  - un radar par système,
  - des recommandations associées.

Étape 3 – Ancrer la grille dans différents processus

Par exemple :

- **Processus projets** : niveau AIA-RL_min requis pour passer certains gates.
- **Processus risques / compliance** : utilisation de GovRL / SecRL pour décider du niveau d'examen requis.
- **Processus architecture / IT** : OpsRL comme critère d'acceptation pour déploiement sur certaines plateformes.

Étape 4 – Étendre, automatiser, affiner

- Étendre progressivement le périmètre (systèmes IA supplémentaires).
- Automatiser ce qui peut l'être (découverte d'assets, recueil d'information, dashboards).
- Affiner les grilles, pondérations, seuils en fonction du retour terrain.

Conclusion

Cette veille met en lumière un paysage déjà riche en frameworks (TRL, DRL, MLTRL, MLSMM, ISO 42001, NIST AI RMF, AISPM, MLOps...). Intégrer les assets IA peut être éxécuté en réorganisant ces briques dans une grille de lecture commune, en créant un langage partagé entre métiers, tech, risques, juridique, direction et en ancrant les décisions IA sur une vision claire de la maturité réelle des assets qui les supportent.

La grille de maturité des assets IA, telle que présentée ici, doit être vue comme un instrument interne et modulable, une interface entre des référentiels existants, et un levier de pilotage plus qu'un outil de contrôle.

Elle ne promet ni que tous les systèmes atteindront un jour un niveau 4–5, ni que les organisations doivent investir des montants démesurés pour chaque cas d'usage. Elle propose de concentrer les efforts là où la combinaison valeur / risque le justifie, de rendre explicite ce qui, aujourd'hui, est souvent géré "au feeling" par quelques experts et d'offrir aux décideurs une structure pour chiffrer, prioriser et séquencer les investissements IA.

Eric Blaudez - AI Architect | Responsible AI · AI Act · AI Governance | Bringing R&D AI to Production (TRL 3→6) | EU & Sovereign Programs

La maturité IA des actifs