NEXIALOG CONSULTING

Finance Innovation

FONDATIONS ET GOUVERNANCE POUR UNE

INTELLIGENCE ARTIFICIELLE (IA) DE CONFIANCE

MARS 2026

ÉDITO

L'INTELLIGENCE ARTIFICIELLE, NOUVEAU PILIER DE LA RÉSILIENCE OPÉRATIONNELLE

> « L'IA EST UN ACCÉLÉRATEUR D'EXPERTISE, MAIS SA FIABILITÉ DÉPEND EXCLUSIVEMENT DE LA QUALITÉ DE LA DONNÉE ET DE LA MAÎTRISE DE SES FONDATIONS. »

L'intelligence artificielle n'est plus une option pour les trois lignes de défense : elle en redéfinit déjà les équilibres, les responsabilités et les leviers de performance.

Les métiers du contrôle, des risques, de la conformité et de l'audit vivent une transformation d'une intensité inédite. En quelques mois, l'IA est passée du stade de curiosité technologique à celui d'enjeu structurel. Les organisations avancent désormais sous une double contrainte : répondre à une pression réglementaire croissante illustrée par l'IA Act tout en saisissant l'opportunité de l'IA pour décupler l'efficacité, la résilience et la capacité d'anticipation des dispositifs de contrôle.

DE L'EXPÉRIMENTATION À LA MAÎTRISE SYSTÉMIQUE

La question n'est plus de savoir s'il faut franchir le pas, mais comment le faire avec audace et méthode.

COMMENT INDUSTRIALISER SANS PERDRE LE CONTRÔLE ?
COMMENT PASSER DE POC ISOLÉS À UN DÉPLOIEMENT SYSTÉMIQUE CRÉATEUR DE VALEUR ?

Au fil de nos analyses et des échanges menés avec des experts métiers, des acteurs RegTech et DataTech, un constat s'impose : la différence ne se joue plus sur l'identification des cas d'usage, mais sur la maturité des fondations. Architecture intégrée, gouvernance rigoureuse des données, feuille de route stratégique, cadre d'IA responsable et culture d'adoption : sans ces piliers, l'IA reste périphérique et sa valeur, marginale.

LA DONNÉE : CARBURANT DE LA CONFIANCE

L'IA est puissante, mais sa fiabilité dépend exclusivement de la qualité de la donnée qui l'alimente. Dans les trois lignes de défense, cette donnée transite massivement par des processus documentaires complexes et souvent silotés. Automatiser et industrialiser ces flux, c'est non seulement améliorer la qualité de l'information, mais aussi renforcer la traçabilité et sécuriser les contrôles dans un environnement de plus en plus volatil.

Au cœur de cette mutation, la donnée n'est plus seulement un actif technologique, c'est une responsabilité critique. La pression accrue sur la qualité des données ne tolère plus l'approximation; elle exige une excellence opérationnelle sans faille.

L'HUMAIN AU CŒUR DU DISPOSITIF

Cette transformation, bien que technologique, reste profondément humaine. L'IA n'est pas un substitut à l'expertise : elle en est l'accélérateur et l'amplificateur. Elle libère les équipes des tâches chronophages pour les repositionner sur des analyses à haute valeur ajoutée. Former les collaborateurs, décrypter les limites des modèles, maintenir un regard critique et garantir une supervision constante sont les conditions sine qua non d'une IA de confiance. Le succès repose sur notre capacité à hybrider l'intelligence humaine et artificielle.

UN PAYSAGE DE RISQUES EN MUTATION

L'actualité nous impose une vigilance renforcée. L'IA accélère et amplifie des risques déjà présents, en particulier en matière de cybercriminalité et de fraude. Les deepfakes et l'ingénierie sociale automatisée permettent désormais de mener des attaques massives, rapides et très crédibles. Face à cette industrialisation de la menace, seule une défense elle-même augmentée par l'IA peut réagir en temps réel.

Le risque de blanchiment et de financement du terrorisme évolue lui aussi. La complexité croissante des circuits financiers et le développement des crypto-actifs rendent les dispositifs de contrôle traditionnels insuffisants. Dans ce contexte, la capacité à détecter des schémas inhabituels grâce à l'analyse de données devient un levier central.

Ces transformations dépassent le seul enjeu opérationnel. Dans un environnement international instable, les questions de géopolitique et de souveraineté numérique s'imposent. Maîtriser ses propres modèles d'IA est désormais un choix stratégique. Une dépendance excessive à des solutions externes expose à des risques de rupture de service ou d'atteinte à l'intégrité des données.

La résilience de nos organisations ne reposera donc pas uniquement sur la performance technologique, mais sur notre capacité à garantir la sécurité et l'indépendance de nos systèmes face à des menaces de plus en plus hybrides.

NOTRE AMBITION

Ce livre blanc propose une lecture claire et pragmatique de cette mutation. Structuré autour des trois lignes de défense, il combine analyse réglementaire, benchmark des meilleures pratiques du secteur financier (AML, fraude, cyber) et retours d'expérience concrets.

Notre objectif est d'offrir aux dirigeants et experts une boussole stratégique pour dessiner une trajectoire réaliste et ambitieuse à l'horizon 2030. L'enjeu n'est plus de tester l'IA, mais de l'ancrer durablement au cœur d'un dispositif de contrôle renforcé, responsable et pérenne.

Otman **IBNLKHAYAT**

Senior Manager, Finance, Control & Compliance

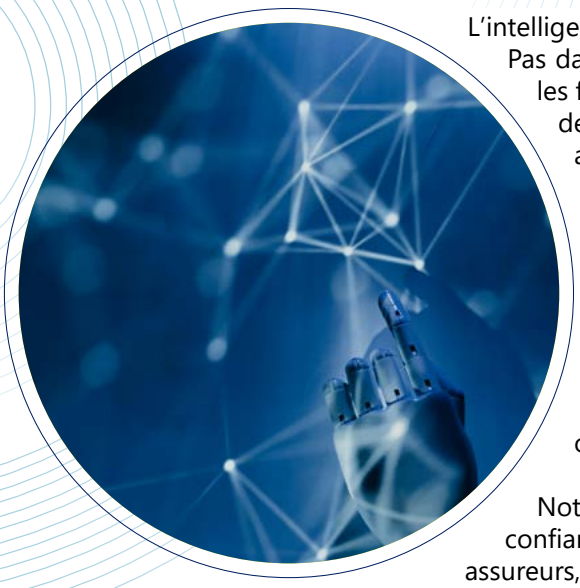
Maïmouna **TOURE**

Expert, Finance, Control & Compliance

El Mehdi **LAALEJ**

Expert, Finance, Control & Compliance

ÉDITO



L'intelligence artificielle transforme déjà le secteur financier en profondeur. Pas dans un futur proche — maintenant. Dans les salles de marchés, les fonctions de conformité, les processus de souscription, les outils de détection des fraudes. Cette réalité, nous la vivons au quotidien au contact de nos membres.

Ce qui me frappe, c'est moins la vitesse de cette transformation que la façon dont elle révèle les fractures de notre écosystème : entre ceux qui avancent vite et ceux qui peinent à suivre, entre l'enthousiasme de l'innovation et la rigueur qu'exige la responsabilité, entre la promesse technologique et la réalité opérationnelle. C'est précisément dans ces espaces de tension que Finance Innovation a un rôle à jouer — pas comme observateur, mais comme catalyseur.

Notre conviction est simple : l'IA ne peut devenir un levier de confiance que si elle est construite collectivement. Banques, fintechs, assureurs, régulateurs — personne ne peut y arriver seul. Les fintechs apportent l'agilité et la capacité d'expérimentation ; les institutions financières, la profondeur métier et l'exigence de robustesse ; les régulateurs, le cadre sans lequel aucun déploiement à grande échelle n'est viable. Notre rôle est de faire travailler ces mondes ensemble, avec exigence et sans naïveté.

Les cas d'usage réunis dans ce livre blanc sont le fruit de cette collaboration. Ils ne sont pas des démonstrations — ce sont des résultats. Ils montrent que performance et responsabilité ne s'opposent pas, à condition d'adopter une approche rigoureuse : tester, mesurer, corriger, déployer. Et surtout, partager les enseignements — y compris les difficultés.

Je le dis avec franchise : les risques liés à l'IA sont sérieux. Biais, opacité, dépendances technologiques, responsabilité juridique — ces enjeux ne se résolvent pas avec de bonnes intentions. Ils appellent une gouvernance robuste, un dialogue ouvert et une volonté collective de ne pas sacrifier la résilience au profit de la vitesse.

C'est l'ambition que je porte avec les équipes de Finance Innovation, et que je souhaite voir partagée bien au-delà de nos murs.

Elodie **TREVILLOT**

Présidente, Finance Innovation
Associé-Gérant, Delubac & Cie

A PROPOS DE

Finance Innovation

ACCOMPAGNER ET DÉVELOPPER LA FINANCE DE DEMAIN

Pôle de compétitivité mondial créé par l'Etat en 2007, Finance Innovation dispose d'une légitimité naturelle pour permettre le développement de l'écosystème financier de manière rigoureuse et désintéressée. Alliant la force de son label d'Etat au dynamisme de ses équipes, le pôle est le garant d'un accompagnement de qualité en mettant en relation les start-up, laboratoires de recherche, petites, moyennes et grandes entreprises, centres d'excellence académiques et investisseurs.

- Monter des projets de R&D en finance digitale (EU)
- Identifier et accélérer les Fintechs et leurs projets innovants
- Contribuer à la transformation digitale et durable de la finance et de l'économie

SOMMAIRE

01.

INTRODUCTION

Finance Innovation

NEXIALOG CONSULTING

INTRODUCTION

Les banques et assurances évoluent aujourd'hui dans un environnement de rupture. Mutations réglementaires accélérées, transformation digitale profonde, volatilité économique : autant de facteurs qui redéfinissent les règles du jeu concurrentiel. Dans ce contexte, la conformité n'est plus une simple contrainte administrative. Elle devient un impératif stratégique, au cœur de la compétitivité et de la pérennité des institutions financières.

Le paradoxe est brutal : il faut faire plus, plus vite, avec moins de marge d'erreur. Garantir une conformité irréprochable tout en préservant l'agilité opérationnelle. Maîtriser des risques de plus en plus complexes : cyber, climatiques...tout en maintenant la rentabilité.

Face à ce défi, les dispositifs classiques de contrôle et d'audit prouvent leur inadéquation.

Les fonctions de contrôle interne, de conformité et d'audit sont contraintes de se réinventer, non plus pour constater les anomalies, mais pour les anticiper, non plus pour surveiller, mais pour piloter.

C'est là qu'intervient l'intelligence artificielle (IA) comme nouveau moteur de transformation offrant des capacités inédites :

- Détection en temps réel des fraudes
- Automatisation intelligente des contrôles
- Analyse prédictive des risques
- Veille réglementaire augmentée.

Elle redessine le périmètre d'action des trois lignes de défense (contrôle métier, gestion des risques / conformité et audit interne). Elle fait basculer les institutions d'une posture défensive à une logique d'anticipation stratégique.

L'IA, une opportunité à double tranchant ce n'est pas une baguette magique, son intégration expose les institutions à de nouveaux risques de gouvernance, d'éthique et de responsabilité.

COMMENT GARANTIR LA TRANSPARENCE DES ALGORITHMES ?
COMMENT ÉVITER LES BIAIS DISCRIMINATOIRES ?
COMMENT PRÉSERVER LE JUGEMENT HUMAIN ?
COMMENT SE CONFORMER À L'IA ACT EUROPÉEN ?

LA QUESTION N'EST PLUS FAUT-IL INTÉGRER L'IA ? MAIS COMMENT L'INTÉGRER INTELLIGEMMENT ?

Face à tous ces constats, une question s'impose : Comment les institutions f inancières peuvent-elles intégrer l'IA dans leurs dispositifs de contrôle interne, conformité et d'audit, tout en conciliant efficacité opérationnelle, exigences réglementaires et impératifs éthiques ? Cette problématique guide l'ensemble de ce livre blanc.

02.

ENTRE INNOVATION ET CONFORMITÉ : COMPRENDRE LA STRATÉGIE DE L'IA ACT

Finance Innovation

NEXIALOG CONSULTING

L'ENVIRONNEMENT RÉGLEMENTAIRE EN MUTATION

L'essor accéléré de l'IA redéfinit profondément les pratiques de contrôle, de gestion des risques et de conformité. Entre opportunités d'efficacité opérationnelle et impératifs de maîtrise, les établissements financiers doivent naviguer dans un paysage réglementaire en pleine mutation.

L'IA Act, les nouvelles règles de gouvernance des modèles, et les obligations renforcées en matière d'explicabilité ou de gestion des risques imposent une transformation profonde. Ce chapitre éclaire les fondations réglementaires et technologiques indispensables pour comprendre le rôle stratégique de l'IA

IA ACT EUROPÉEN : CLASSIFICATION DES SYSTÈMES ET OBLIGATIONS (2025-2027)

Adopté le 1er août 2024, le Règlement européen sur l'intelligence artificielle (IA Act) constitue le premier cadre législatif transversal dédié à l'intelligence artificielle au niveau mondial. Créer pour concilier protection des droits fondamentaux, sécurité, valeurs européennes et innovation, il prolonge la stratégie d'une IA « digne de confiance » et s'inscrit dans la continuité du marché unique numérique.

Le texte introduit une approche par niveau de risque, encadrée par un dispositif de conformité, contrôle, gouvernance et sanctions, et assortie d'une période transitoire de 24 mois.

- Les obligations relatives à la sensibilisation et aux systèmes interdits s'appliquent depuis février 2025.
- Les exigences destinées aux fournisseurs et déployeurs de systèmes d'IA à haut risque et aux obligations de transparence entreront en vigueur à partir du 2 août 2026.

LE RÈGLEMENT VISE TROIS FINALITÉS

- protection des droits fondamentaux ;
- soutien à une innovation responsable et encadrée ;
- création d'un marché unique de l'IA compétitif et cohérent.

SES AXES STRATÉGIQUES PORTENT SUR

- une IA éthique et centrée sur l'humain ;
- l'harmonisation réglementaire en Europe ;
- le soutien à l'innovation.

Le texte* comprend : 180 considérants, 113 articles (13 chapitres), 13 annexes, 68 définitions, 144 pages. La mise en œuvre sera complétée par les avis du Comité européen de l'IA.

Le champ d'application couvre tous les systèmes et modèles d'IA, y compris hors UE dès lors qu'ils produisent un effet dans l'Union. Tous les acteurs de la chaîne de valeur sont concernés : fournisseurs, utilisateurs/déployeurs, importateurs, distributeurs, développeurs de modèles d'IA à usage général.

PRINCIPALES EXIGENCES

- Acculturation obligatoire pour assurer un niveau suffisant de maîtrise (art. 4).
- Interdiction et suppression des systèmes prohibés (art. 5).
- Pour les systèmes à haut risque : obligations strictes, conformité renforcée, documentation, surveillance, auditabilité.
- Sanctions pouvant atteindre 35 M€ ou 7 % du CA mondial.

L'IA ACT AJOUTE UNE CLASSIFICATION PAR RISQUE

Figure 2.1

**Règlement - UE - 2024/1689 - EN - EUR-Lex*

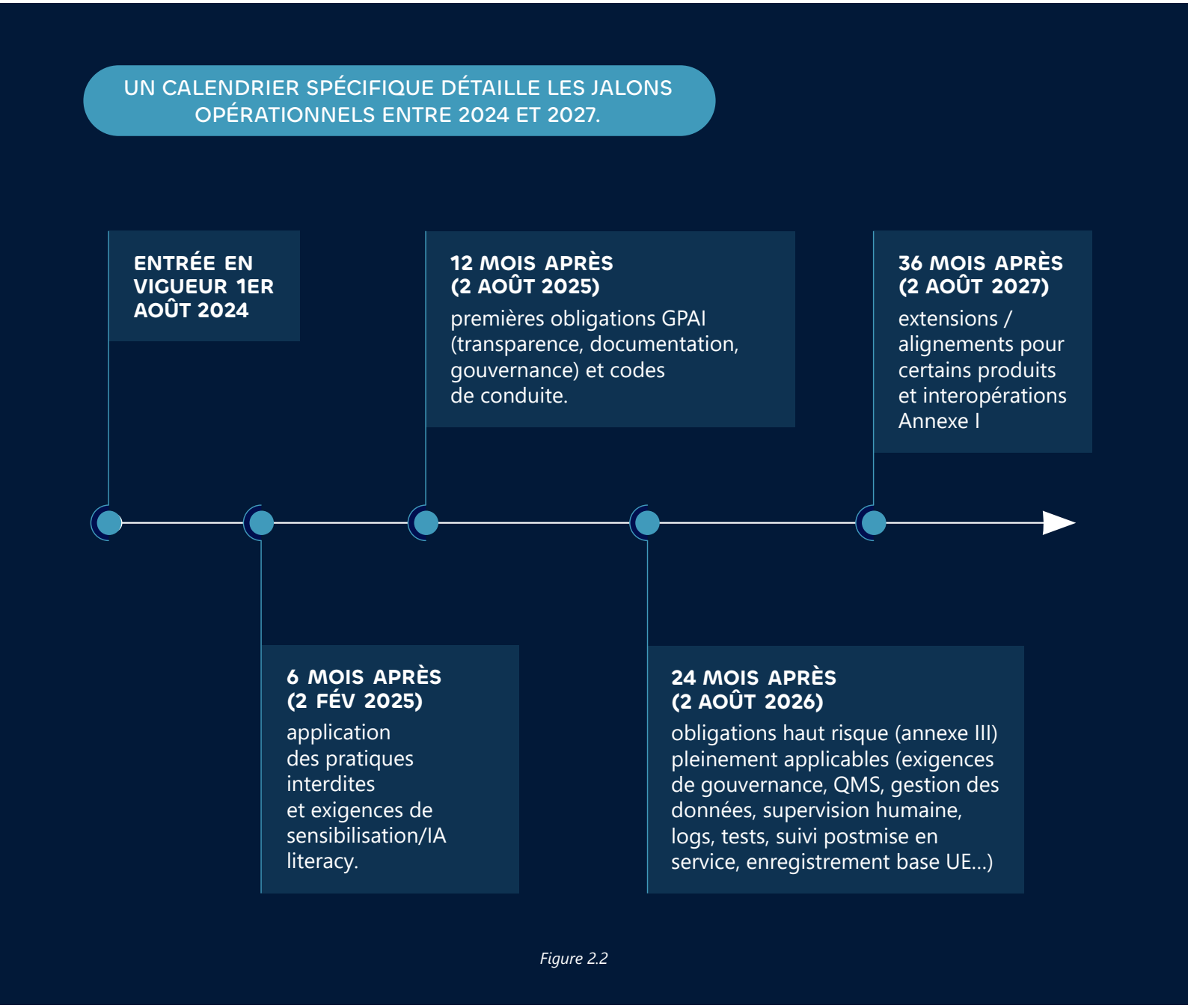


Figure 2.2

Au-delà du calendrier IA Act, les régulateurs sectoriels précisent de plus en plus les attentes opérationnelles. Ces lignes directrices traduisent les principes du règlement en pratiques de gouvernance, de documentation et de surveillance des modèles. Elles visent surtout à harmoniser les exigences de contrôle, de traçabilité et de maîtrise des risques liés à l'usage de l'IA.

GUIDELINES SECTORIELLES : EBA/BCE (BANQUE), AMF/ESMA (FINANCE), EIOPA (ASSURANCE)

LES RÉGULATEURS SECTORIELS CONVERGENT SUR PLUSIEURS EXIGENCES

- Gouvernance des modèles,
- Traçabilité et explicabilité,
- Qualité des données,
- Gestion des tiers (outsourcing, cloud),
- Surveillance continue (LOD1/LOD2/LOD3).

Toute utilisation de modèles fournis par des tiers (scoring, fraude…) impose à l'établissement d'être capable de comprendre, contrôler et auditer les modèles (ex. : guidelines EBA/GL/2019/02).

Les autorités EBA, ESMA, EIOPA coordonnent l'application cohérente de l'IA Act dans leurs secteurs, ce qui renforce l'harmonisation réglementaire.

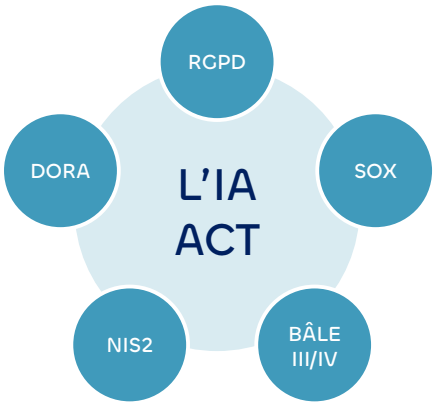


Figure 2.3

ARTICULATION AVEC RGPD, SOX, BÂLE III/IV, NIS2, DORA

L'IA Act s'ajoute à un environnement déjà dense, sans alléger les obligations existantes. Le RGPD reste pleinement applicable : base légale, principes de licéité et transparence, minimisation, droits des personnes. La DPIA (article 35 RGPD) demeure obligatoire pour les traitements à risque élevé, tandis que le IA Act impose des évaluations d'impact sur les droits fondamentaux (FRIA) pour les systèmes d'IA à haut risque.

Le règlement DORA (janvier 2025) complète le IA Act sur la résilience opérationnelle, la gestion des risques TIC, la supervision des prestataires tiers critiques et les tests de résilience.

Les systèmes d'IA utilisés dans les infrastructures critiques doivent donc répondre simultanément :

- Aux exigences techniques du IA Act (documentation, explicabilité, monitoring) ;
- Aux obligations de DORA (incidents, continuité, cyber-tests).

Les dispositifs doivent aussi s'articuler avec MiFID II/ESMA, AML/CFT, NIS2.

Ces exigences s'appliquent à toutes les technologies d'IA utilisées dans la finance : machine learning, NLP, réseaux de neurones, etc.

Les principaux défis réglementaires de l'IA Act applicables aux institutions financières et aux secteurs RegTech sont la conformité multi-cadres (IA Act, RGPD, DORA et autres normes), la classification des risques des modèles d'IA, la traçabilité et l'explicabilité des algorithmes, la gestion des données et des tiers, et la responsabilité légale en cas d'échec.

Cela présente un double dilemme : assurer la conformité tout en soutenant l'innovation et l'agilité. Le succès repose sur : une structure de gouvernance interne solide ; des compétences appropriées ; des partenariats clairs avec les fournisseurs ; et une perspective à long terme pour la conformité de l'IA.

DÉCLINAISON DE L'IMPACT DE L'IA ACT SUR LES TROIS LIGNES DE DÉFENSE

À travers une analyse fine de l'IA Act, l'analyse ci-dessous présente une gap analysis des impacts de la réglementation sur les trois lignes de défense et évalue le niveau de conformité actuel au regard des principales exigences réglementaire

L'objectif est d'identifier les obligations applicables, leurs impacts métiers et le niveau de couverture, tout en mettant en évidence les actions à mener pour aligner les pratiques internes avec la réglementation.

TABLEAU

Elle clarifie enfin la répartition des responsabilités entre les différentes lignes de défense et constitue un support de pilotage pour structurer priorités, contrôles et plans d'amélioration.

Ce tableau sert ainsi de support de pilotage pour la mise en conformité à l'IA Act, en structurant les priorités, les contrôles et les améliorations à mettre en place.

EXIGENCE IA ACT	ARTICLE	LOD CONCERNÉ	IMPACT MÉTIER	NIVEAU OBSERVÉ	CONSTAT MARCHÉ	PRIORITÉ
Maîtrise IA	Art. 4	LOD 1	Formation obligatoire des équipes, certification utilisateurs IA	🔴	La majorité des organisations n'ont pas de programme formel D'IA.	P1
Pratiques interdites	Art. 5	LOD 1	Identification et blocage des usages prohibés (scoring social, manipulation, etc.)	🟡	Contrôles existants mais dépendance à l'auto-déclaration	P1
Qualification systèmes haut risque	Art. 6 & Annexe III	LOD 2/3	Méthodologie de classification des systèmes IA selon niveau de risque	🟠	Qualification réalisée mais peu documentée	P1
Gestion risques IA	Art. 9	LOD 2/3	Registre des risques IA spécifiques (biais, dérive, hallucinations)	🟠	Registre des risques IT général étendu à l'IA. Risques spécifiques (biais algorithmiques, adversarial attacks, dérive) peu documentés. Absence de méthode IA dédiée.	P1
Gouvernance données	Art. 10	LOD 2/3	Qualité, représentativité et détection des biais dans les jeux de données	🟠	Contrôles qualité données traditionnels (complétude, cohérence) mais tests de représentativité et détection automatique des biais quasi inexistants.	P1
Documentation technique	Art. 11	LOD 2/3	Dossier technique structuré conforme Annexe IV (specs, tests, limites, données)	🟠	Documentation dispersée dans outils multiples (Confluence, SharePoint, Jira). Pas de dossier centralisé par système IA. Format Annexe IV inconnu des équipes.	P1
Logs & traçabilité	Art. 12	LOD 1/2/3	Traçabilité opérationnelle des systèmes IA	🟡	Logs techniques présents mais politique de rétention floue, absence de procédures de restitution formalisées. Logs modifiables a posteriori.	P1
Transparence utilisateurs	Art. 13	LOD 1	Information claire sur l'usage d'IA et les limites	🟠	Informations non homogènes selon les usages	P2
Supervision humaine	Art. 14	LOD 1/2	Organisation des rôles, procédures d'override	🟠	Validation humaine existe pour décisions critiques mais procédure d'override non formalisée.	P1
Robustesse & cybersécurité	Art. 15	LOD 2/3	Tests performance, résistance attaques, détection dérive modèle	🟠	Tests au déploiement (accuracy, latence) mais monitoring dérive absent. Tests adversariaux jamais réalisés. Prompt injection non testée.	P1
Obligations fournisseurs	Art. 16	LOD 2	Clauses contractuelles IA Act : docs, logs, audits, délais incidents	🔴	Contrats standard IT sans clauses IA Act spécifiques. Aucun droit d'audit IA formalisé ni d'obligations de due diligence fournisseurs IA.	P1
QMS IA (système qualité)	Art. 17	LOD 2/3	Processus qualité dédié IA : conception, validation, changements, audits	🔴	Pas de QMS dédié à L'IA.	P2
Conservation documentaire	Art. 18-19	LOD 2/3	Preuves réglementaires conservées 10 ans	🟠	Archivage existant mais non aligné IA Act	P2
Chaîne de valeur (tiers)	Art. 23-25	LOD 2	Cartographie responsabilités fournisseurs/intégrateurs/distributeurs IA	🔴	Responsabilités insuffisamment cartographies	P1
Obligations déployeurs	Art. 26	LOD 1	Surveillance opérationnelle : KPIs, alertes, revues périodiques	🟠	Utilisation quotidienne maîtrisée mais KPIs IA Act absents (taux erreur, interventions humaines, plaintes). Revues périodiques inexistantes ou informelles (emails).	P1
FRIA (droits fondamentaux)	Art. 27	LOD 1/2	Évaluation impact sur vie privée, non-discrimination, transparence, recours	🔴	Évaluations d'impact non réalisées. DPIA (RGPD) parfois confondue avec FRIA. Aucune méthode standardisée.	P1
Transparence deepfakes	Art. 50	LOD 1	Mention explicite «généré par IA» sur contenus synthétiques	🟠	Obligations comprises pour chatbots (70% compliance) mais contenus génératifs (images, vidéos) rarement labellisés. Watermarking IA quasi absent. Risque réputationnel sous-estimé.	P2
GPAI (modèles génériques)	Art. 53 & 55	LOD 2	Exigences contractuelles envers fournisseurs OpenAI, Anthropic, etc.	🔴	Dépendance critique à GPAI commerciaux (ChatGPT, Claude) sans clauses IA Act. Utilisation d'APIs sans documentation modèle, politique copyright, évaluation risques systémiques.	P1
Surveillance post-marché	Art. 72	LOD 1/2/3	Monitoring continu + reporting régulateur (si applicable)	🟠	Monitoring existant mais non structuré IA Act	P1
Incidents graves	Art. 73	LOD 1/2/3	Process escalade + déclaration autorités sous 15 jours calendaires	🔴	Process incidents IT généraux (SLA 24-72h) inadaptés aux délais IA Act (15j). Absence de classification «incident grave IA». 90% organisations ne peuvent pas respecter deadline réglementaire.	P1

Tableau 2.1

RECOMMENDATIONS CLÉS

1. **INVENTAIRE EXHAUSTIF DES USAGES IA :**
Développés en interne ou intégrés à des solutions du marché, qu'ils soient en production ou en cours de déploiement. Ce travail d'inventaire doit se faire auprès de tous les métiers au moyen de questionnaires ou des entretiens cibles.

2. **CLASSIFICATION PAR CRITICITÉ ET CONFORMITÉ :**
Ces actions permettront d'alimenter un registre des SIA (point d'entrée et le suivi global des risques), les éléments qui devront figurer dans ce registre incluent :
   - Les sources de données (origine des données, méthode de collecte, de nettoyage…)
   - Les architectures techniques (infrastructures cloud utilisés)
   - Les cas d'usages métier avec les objectifs, les bénéfices attendues
   - Le contexte de déploiement ou d'usage

3. **MISE EN PLACE D'UNE GOUVERNANCE DÉDIÉE :**
Mettre en place une gouvernance claire pour la surveillance de l'IA, en définissant et attribuant les rôles et responsabilités sur la législation européenne sur l'IA et les pratiques d'IA responsable.

4. **FORMATION DES ÉQUIPES :**
L'article 4 de l'IA Act impose à toutes les organisations qui déploient ou utilisent des systèmes d'IA de développer une littératie numérique sur l'IA de ses risques auprès des employés pour garantir une maîtrise suffisante (formation au fonctionnement et aux risques, développement des compétences techniques…).

5. **OUTILS DE MONITORING ET D'EXPLICABILITÉ :**
(Data & IA Ethique, évaluation de SIA, procédures d'explicabilité et de constabilité…).

6. **DOCUMENTATION RIGOUREUSE :**
Définir et partager des procédures d'évaluation, de mitigation et de contrôle des risques.

7. **DIALOGUE PRÉCOCE AVEC LES SUPERVISEURS.**

8. **ANTICIPATION DES FUTURES ÉVOLUTIONS RÉGLEMENTAIRES :**
De la manière dont l'IA est adoptée dans l'organisation et des impacts qu'elle a déjà sur l'organisation, ses parties prenantes interne et externe. Assurer une veille réglementaire pour saisir les bonnes pratiques et les intégrer.

Face aux exigences du Règlement (UE) 2024/1689 (“IA Act”), Nexialog accompagne les organisations dans la mise en conformité de leurs dispositifs de contrôle interne, de conformité et d’audit. Grâce à notre expertise Finance, Control & Compliance, nous aidons à structurer les cadres de gouvernance nécessaires : documentation et traçabilité des systèmes d’IA, dispositifs de supervision humaine, processus de gestion des risques et exigences de contrôle renforcé, tels que définis par le règlement européen.

En complément, notre savoir-faire Data Consulting permet de sécuriser l’ensemble de la chaîne de traitement des données et des modèles : préparation, normalisation, contrôle, monitoring et mise en production afin d’aligner les pratiques opérationnelles sur les obligations de qualité, de robustesse et de transparence imposées par le IA Act.

En combinant maîtrise réglementaire et expertise technique, nous offrons un accompagnement complet pour aider les entreprises à intégrer l’IA dans un cadre maîtrisé, conforme et auditable, en garantissant fiabilité des données, cohérence des processus et conformité aux standards européens.

03.

BATIR LES FONDATIONS : COMMENT UNE GOUVERNANCE ROBUSTE DE LA DONNÉE ACCELERE L'IA

Finance Innovation

NEXIALOG CONSULTING

QUALITÉ, DISPONIBILITÉ, TRAÇABILITÉ, PROTECTION, STRUCTURATION : UNE GOUVERNANCE SOLIDE DE LA DONNÉE CONDITIONNE DIRECTEMENT LA PERTINENCE DES MODÈLES ET LA PERFORMANCE DES OUTILS

Dans le cadre du développement et de l'utilisation des systèmes d'IA, la gestion des données est cruciale. Ces systèmes reposent sur des données qui doivent respecter quatre principes clés : la qualité, la sécurité, la confidentialité et la transparence. Des informations exactes, complètes et régulièrement mises à jour sont importantes pour garantir la qualité des informations depuis la collecte des données jusqu'aux mécanismes de vérification, par des contrôles continus.

La qualité des données doit être garantie par des informations exactes, complètes et régulièrement mises à jour, grâce à des mécanismes de vérification continue.

Leur sécurité exige une protection efficace contre tout accès ou usage non autorisé. Leur confidentialité doit être assurée conformément aux réglementations sur la protection des données personnelles, notamment le règlement RGPD. La transparence exige enfin que les organisations révèlent leur collecte et traitement des données au public en publiant leurs politiques de confidentialité et en établissant des outils de contrôle et d'audit.

La qualité des données fait toutefois déjà l'objet de réglementations spécifiques, notamment dans les secteurs bancaire et assurantiel. Ainsi l'article 82 de la directive 2009/138/CE du Parlement européen et du Conseil (Solvabilité II) établit certaines exigences spécifiques pour les assureurs concernant la fiabilité et l'exhaustivité des données.

Le secteur bancaire également concerné par la norme BCBS 239 établie par le Comité de Bâle sur le contrôle bancaire, qui définit les principes de gouvernance et de gestion des données.

Ces obligations sont également renforcées par le décret du 25 février 2021, qui a modifié le décret du 3 novembre 2014 (article 104) en France. Le principe de qualité des données ne concerne donc pas seulement les modèles d'intelligence artificielle mais s'inscrit également dans une continuité réglementaire existante.

GOUVERNANCE DES DONNÉES

La gouvernance des données est la pierre angulaire pour faciliter l'utilisation éthique, responsable et réglementée des données dans les systèmes d'IA. Elle repose sur un ensemble de politiques et de procédures nécessaires pour protéger l'utilisation de ces informations.

La qualité, la sécurité, la confidentialité et l'intégrité des informations n'est qu'un aspect de leur protection.

Mais cela va au-delà : la gouvernance des données ne s'arrête pas là, il faut également respecter les droits des personnes et les réglementations en vigueur.

L'objectif est simple : Il s'agit de la manière dont ces données sont contrôlées, protégées et maintenues de bonne qualité. Ainsi que la conformité aux cadres légaux.

La gouvernance de donnée vise in fine la fiabilité, l'accessibilité et la protection des informations contre tout risque liés à la sécurité et à l'information.

LES PRINCIPES DE GOUVERNANCE DES DONNÉES

DISPONIBILITÉ ET QUALITÉ DES DONNÉES

Les données nécessaires pour les modèles doivent être examinées durant toutes les étapes de leur cycle de vie.

Dans l'aspect modélisation de la construction du modèle, ce risque survient surtout en raison de données critiques manquantes ou incomplètes, par exemple en raison d'un historique insuffisant ou de contraintes réglementaires limitant les périodes de conservation.

D'autre part, les données peuvent être manquantes, invalides ou disponibles avec un retard pendant la phase opérationnelle (exploitation), ce qui peut nuire la performance du modèle.

En évaluant régulièrement la qualité des données d'entrée pendant le processus de développement et en surveillant la qualité et la disponibilité des données après le déploiement du modèle, ces risques peuvent être minimisés. Par conséquent, ces mesures de contrôle doivent être intégrées dans l'évaluation globale des risques.

LES DONNÉES EXTERNES

Les données externes utilisées par un modèle échappent souvent au contrôle de l'organisation, tant au niveau de leur qualité que de leur méthode de production.

Des risques peuvent alors découler d'un manque de transparence concernant la définition des données, les méthodes de mesure, l'agrégation ou le calcul utilisés. Contrairement aux données internes, dont la qualité est généralement garantie par leurs producteurs.

L'évaluation de la fiabilité des données externes incombe au data scientist ou au propriétaire du modèle. Cette vigilance doit être exercée tant lors de la calibration du modèle que pendant sa phase opérationnelle, afin d'assurer la cohérence et la robustesse des résultats produits.

UTILISATION DE DONNÉE SANS AUTORISATION

Dans le secteur bancaire, les systèmes informatiques traitent une volumétrie importante des données sensibles. C'est la raison pour laquelle Le RGPD impose un cadre strict pour encadrer leur utilisation.

Dans certains cas, le consentement des personnes concernées est obligatoire et doit être lié à des finalités clairement définies.

L'utilisation d'un modèle doit respecter ces finalités pour éviter tout usage abusif des données.

L'exploitation de données historiques soulève des risques spécifiques, notamment lorsque la période de conservation réglementaire est dépassée ou que le droit à l'oubli s'applique. Ces contraintes peuvent créer des difficultés pour harmoniser les réglementations locales avec le cadre européen. Elles concernent aussi bien les données individuelles que les traceurs comme les cookies.

Ces risques méritent d'être pris en compte dès le début du développement des ensembles de données, soumis à un régime de gouvernance strict comprenant à la fois les data scientists et ceux qui sont tenus de respecter la conformité au traitement des données personnelles (DPO).

ANONYMISATION DES DONNÉES

La norme internationale ISO/IEC 29100 : 2011 définit l'anonymisation comme un processus irréversible rendant impossible l'identification des personnes concernées. Tandis que la pseudonymisation utilise des codes qui permettent de retrouver l'identité avec une clé. Pour créer des modèles, l'anonymisation est recommandée car elle offre la meilleure protection. Toutefois, si elle supprime trop d'informations utiles, la pseudonymisation peut être utilisée, à condition de respecter le RGPD et le consentement des personnes.

PROTECTION DES DONNÉES

Pour les institutions financières, la protection des données personnelles et sensibles est fondamentale. Néanmoins, l'IA peut fragiliser cette protection. L'IA présente plusieurs risques :

- Piratage du modèle
- Attaques sur les outils d'entraînement
- Fuites de données

C'est pourquoi il faut sécuriser le modèle à chaque étape, de sa création à son utilisation.

PRÉ-TRAITEMENT DE DONNÉES

DONNÉES INCOMPLÈTES OU BIAISÉES

Les données d'IA peuvent contenir des erreurs ou des biais dus à des informations incomplètes, des historiques imparfaits ou des erreurs de traitement. Ces défauts risquent de fausser les résultats du modèle. Enfin, des erreurs de prétraitement comme une catégorisation, une labellisation ou une normalisation incorrecte peuvent accentuer ces déséquilibres et compromettre la fiabilité du modèle.

Donc il est essentiel de contrôler rigoureusement la qualité des données à chaque étape, de la création à l'utilisation du modèle.

DONNÉES SENSIBLES

Le choix des données intégrées dans un modèle constitue une étape critique, car certaines variables peuvent introduire des biais ou des discriminations. Des attributs tels que le genre ou l'âge sont particulièrement sensibles et font l'objet d'un encadrement strict par le RGPD, qui définit une liste de données sensibles dont l'usage est, en principe, interdit.

Il appartient donc au Model Owner et au Model Developer de maîtriser les variables utilisées et de s'assurer qu'aucune donnée non tolérée ne soit intégrée comme variable d'entrée directe.

Certaines exceptions existent toutefois, notamment dans le domaine de l'assurance, où l'âge peut être pris en compte lorsqu'il constitue un facteur de risque objectivement justifié.

L'exploitation de données sensibles, même dans un cadre légal, expose les organisations à des risques réglementaires et de réputation élevée, et nécessite une justification documentée et proportionnée à la f inalité du modèle.

DÉFIS ET SOLUTION

Gérer les données devient de plus en plus complexe : leur volume explose, leur protection est cruciale, et les règles changent régulièrement. Pour relever ces défis, les entreprises doivent s'équiper d'outils adaptés et définir des politiques strictes.

UTILISATION DES TECHNOLOGIES AVANCÉES

Pour renforcer la gestion de l'information, plusieurs solutions s'offrent aux organisations financières :

- Le cloud permet de centraliser et d'organiser les informations, tout en offrant un stockage et un traitement sécurisés à grande échelle.
- Le chiffrement, l'authentification à double facteurs et la gestion des clés de sécurité aident à garantir une protection renforcée et une conformité optimale.
- L'edge computing constitue également une approche complémentaire, consistant à traiter les données localement avant leur transfert vers des centres de données centralisés.

FORMATION ET SENSIBILISATION DES EMPLOYÉS

La formation des employés est essentielle pour garantir une bonne gouvernance des données. Plusieurs actions peuvent être mises en place :

- **Développer une culture data et clarifier la gouvernance :**
  La maîtrise des rôles et responsabilités (Data Owner, contributeurs métiers) constitue le socle d'une gouvernance efficace. La formation doit clarifier le périmètre d'intervention de chaque acteur.
- **Garantir la qualité et la fiabilité des données :**
  La formation doit couvrir les contrôles de qualité, la gestion des anomalies et le pilotage par indicateurs pour assurer des données fiables et exploitables.
- **Assurer la conformité réglementaire et l'éthique des usages :**
  Au-delà du RGPD et des réglementations sectorielles, la sensibilisation doit porter sur les principes de minimisation, de conservation proportionnée et de confidentialité. La prévention des biais algorithmiques et l'usage responsable de la donnée s'affirment comme des enjeux majeurs dans les secteurs régulés.
- **Sécuriser les actifs data et prévenir les risques :**
  La protection exige une approche globale : classification rigoureuse, gestion des habilitations, chiffrement et prévention des fuites. La sensibilisation aux menaces courantes (phishing, mots de passe, ingénierie sociale) demeure indispensable, le facteur humain représentant un vecteur de risque significatif.
- **Tester les dispositifs et ancrer l'amélioration continue :**
  Les exercices de simulation d'incidents permettent d'évaluer la réactivité organisationnelle et de clarifier les procédures d'escalade. Ces mises en situation révèlent les points de friction et alimentent une démarche d'amélioration continue.

La donnée devient un avantage compétitif, à condition d'être orchestrée avec rigueur. Une gouvernance robuste accélère l'adoption, sécurise les modèles et permet de maximiser la valeur. Sans ces fondations, même les technologies les plus avancées restent sous-exploitées.

La gouvernance des données, aussi structurée soit-elle, doit absolument s'incarner dans un dispositif de contrôle adapté aux spécificités de l'IA.

Le modèle des trois lignes de défense, socle du dispositif de maîtrise des risques bancaires et assurantiels, connaît une mutation profonde.

L'IA ne se contente plus d'être un simple objet de contrôle, elle devient également un outil de contrôle, transformant radicalement les rôles et responsabilités de chaque ligne.

La gouvernance, la qualité, la sécurité et la conformité des données constituent le socle de l'efficacité opérationnelle. Dans la suite de ce livre blanc, vous découvrirez des cas d'usage concrets illustrant comment les trois lignes de défense appliquent ce modèle de gouvernance dans leurs activités quotidiennes.

Notre cabinet mobilise son expertise Data Consulting pour renforcer la gouvernance et la qualité des données au sein des environnements soumis à des exigences élevées de contrôle interne, de conformité et d'audit. Notre intervention couvre l'ensemble de la chaîne data : préparation, normalisation, contrôle, gestion des référentiels, structuration des pipelines, monitoring et industrialisation. Cette maîtrise end-to-end permet d'implémenter des cadres de gouvernance alignés sur les standards réglementaires, d'améliorer la fiabilité et la traçabilité des jeux de données, et de sécuriser l'exploitation analytique ou algorithmique — y compris via des modèles de machine learning mis en production dans des environnements contrôlés.

INTERVIEW

Daniel
BENOILID
CEO de Wirk

La start-up Wirk se positionne comme fournisseur de solutions innovantes (SaaS) au service de l'optimisation et de la gestion de flux documentaires entrants. A travers différents modules de pilotage et d'automatisation des traitements documentaires notre solution est déployée notamment dans l'écosystème Banque / Assurance. Plusieurs cas d'usage en production permettent notamment de simplifier et d'améliorer les contrôles KYC (ex : LCB-FT) à la fois sur les personnes physiques et/ou morales.

« L'ENJEU N'EST PLUS SEULEMENT D'AUTOMATISER LA CONFORMITÉ, MAIS DE LA RENDRE STANDARDISÉE, EXPLICABLE ET AUDIT-READY À GRANDE ÉCHELLE. »

QUELS SONT LES PRÉREQUIS ESSENTIELS EN MATIÈRE DE GOUVERNANCE DES DONNÉES POUR UN DÉPLOIEMENT FIABLE DE L'IA ?

La qualité de la donnée entrante a évidemment un impact direct sur la performance des modèles. Toutefois, avec l'émergence des modèles génératifs récents, la dépendance à une connaissance a priori très structurée diminue, notamment grâce à des approches de type zero-shot.

Dans le traitement documentaire, il convient de distinguer deux sujets :

- La lecture du document (qualité du scan, lisibilité), qui relève davantage de problématiques amont que de l'IA elle-même ;
- La compréhension du contexte, l'analyse et l'extraction de l'information, qui relèvent pleinement des modèles d'IA.

Les documents très peu structurés génèrent naturellement des taux de réussite inférieurs à ceux de documents standardisés.

En matière de gouvernance, lors du déploiement chez les clients, des dispositifs d'assurance qualité sont systématiquement mis en place :

- attribution de scores de confiance sur les résultats livrés ;
- mise en œuvre de contrôles additionnels, ponctuels ou systématiques ;
- revue humaine en fonction de seuils définis par le client.

QUELS SONT LES DIFFÉRENTS DÉFIS RENCONTRÉS LORS DU TRAITEMENT MASSIFS DE DONNÉES ?

De manière contre-intuitive, les projets les plus volumineux sont souvent les plus simples à déployer. Les grandes organisations disposent des ressources IT, de chefs de projet dédiés et parfois de cabinets de conseil pour structurer l'intégration.

Les difficultés apparaissent plus fréquemment sur des projets de plus petite taille, où les équipes sont moins structurées et où l'intégration repose sur des ressources disponibles de manière ponctuelle.

Les obstacles sont rarement techniques. Ils sont principalement :

- organisationnels (évolution des processus, impacts RH) ;
- liés à la transformation des modes de travail ;
- liés à la mise en place de nouveaux dispositifs de contrôle qualité et d'audit pour des processus automatisés.

Le passage d'un pilote réussi à une industrialisation reste un enjeu majeur, commun à de nombreux projets technologiques.

QUELS EST LE POSITIONNEMENT WIRK VIS-À-VIS DE L'IA ET LES TECHNOLOGIES UTILISÉES ?

Nous offrons un service opérationnel répondant à des cas d'usage précis (KYC, LCB-FT, contrôle de conformité documentaire).

Aujourd'hui, trois grandes familles de technologies sont utilisées :

1. Modèles supervisés par gabarits – propriétaire et développé par notre équipe
   - Extraction d'informations sur des documents standardisés (pièces d'identité, justificatifs, formulaires) ;
   - Entraînement sur la base d'annotations ;
   - Outils no code permettant aux clients de créer leurs propres gabarits.

2. Modèles de type LLM – Utilisation et customisation de modèles Open-Source
   - Utilisés pour les documents non structurés ;
   - Compréhension du contexte, extraction et structuration de l'information ;
   - Mise à disposition de bacs à sable permettant aux clients de tester différents modèles et de personnaliser les prompts.

3. Contrôle humain optionnel
   - Relecture humaine en fonction de seuils de confiance ;
   - Amélioration de la qualité livrée ;
   - Constitution progressive de bases d'apprentissage lorsque nécessaire.

COMMENT GÉREZ-VOUS LES CAS OÙ LE CLIENT NE DISPOSE PAS D'UN HISTORIQUE SUFFISANT POUR ENTRAÎNER OU CALIBRER LES MODÈLES ?

Lorsque le cas est relativement simple, et qu'un modèle de type LLM est capable de produire une pertinente en zero-shot, il n'est pas nécessaire de disposer d'un historique conséquent. Dans ce cas, l'IA peut être utilisée directement.

En revanche, lorsque le cas est plus complexe et que le client ne dispose pas d'historique, nous proposons généralement une approche hybride combinant IA et contrôle humain.

L'IA réalise une première extraction, puis un opérateur humain contrôle et valide les résultats. Les données validées permettent progressivement de constituer une base d'apprentissage.

Cette approche permet :

- d'obtenir des gains d'efficacité immédiats ;
- de réduire la charge humaine dès le démarrage ;
- d'enrichir progressivement les modèles lorsque le cas d'usage s'y prête.

Il est toutefois important de noter que le surapprentissage n'est pas systématiquement pertinent : selon les cas, il peut n'apporter qu'un gain marginal de qualité.

CAS D'USAGE EN MATIÈRE DE LCB-FT, ET LES RÉSULTATS OBTENUS

Dans le cadre des cinquième et sixième directives européennes LCB-FT, les établissements financiers et assureurs sont tenus d'identifier les bénéficiaires effectifs des personnes morales.

Concrètement, lorsqu'une entreprise ouvre un compte, l'établissement doit être en mesure d'identifier les personnes physiques qui détiennent, directement ou indirectement, le capital ou les droits de vote.

Notre solution repose sur une méthodologie automatisée :

- à partir d'un numéro SIREN, nous collectons en open data l'ensemble des documents relatifs à l'entreprise ;

- ces documents sont analysés afin d'identifier les actionnaires ;
- si l'actionnaire est une personne morale, le processus est réitéré afin de remonter la chaîne de détention jusqu'aux personnes physiques ;
- les participations sont ensuite agrégées afin de consolider les détentions indirectes.

Des mécanismes de rapprochement d'identités (comparaison de noms, distances de similarité) sont utilisés afin de fusionner les participations lorsqu'une même personne apparaît à différents niveaux de la chaîne.

Le livrable transmis au client comprend :

- la liste des bénéficiaires effectifs identifiés ;
- une comparaison éventuelle avec les déclarations enregistrées au greffe, permettant de détecter des écarts ;
- une fiche de synthèse détaillant les diligences réalisées ;
- la liste des documents analysés et les règles métiers appliquées, constituant une preuve d'audit exploitable en cas de contrôle du régulateur.

QUELS EFFETS ORGANISATIONNELS OBSERVÉS SUITE À L'INDUSTRIALISATION DE CES TRAITEMENTS ?

L'un des effets notables est que les résultats produits sont utilisés par un grand nombre d'utilisateurs finaux.

Il arrive que certains collaborateurs remettent en question les résultats, en constatant des différences avec leurs pratiques antérieures. Dans certains cas, cela met en évidence des interprétations locales ou des pratiques non homogènes.

L'industrialisation implique nécessairement une standardisation : il n'est plus possible de traiter chaque dossier de manière totalement individuelle.

> « L'IA N'EST PAS UNE FIN EN SOI : SA VALEUR RÉSIDE DANS SA CAPACITÉ À RENDRE LES PROCESSUS DE CONFORMITÉ ET DE TRAITEMENT DOCUMENTAIRE PLUS FIABLES, PLUS HOMOGÈNES ET AUDITABLES À GRANDE ÉCHELLE. »

Dans des environnements à fort volume, les règles doivent être formalisées, explicites et reproductibles.

Ce travail de formalisation permet également de transformer une expertise individuelle en règles opérationnelles intégrables dans un système automatisé, ce qui constitue un levier important de robustesse et de conformité.

LES OBSTACLES LES PLUS RÉCURRENTS SUR CE TYPE DE DÉPLOIEMENT

Dans ce cas précis, la qualité de l'input n'est pas un obstacle majeur, puisque les documents sont collectés à travers l'open-data directement à partir du numéro SIREN.

La principale difficulté réside dans l'interprétation de la réglementation.

Chaque établissement peut avoir sa propre lecture de certaines situations spécifiques (successions, modalités de détention, proratisation, etc.). Lors de l'implémentation d'un cadre standardisé, il est parfois complexe d'aligner les équipes conformité, les équipes commerciales et les équipes projet afin de définir des règles communes.

L'industrialisation oblige à formaliser et expliciter des règles qui, auparavant, pouvaient être appliquées de manière hétérogène par le réseau.

Cette standardisation est souvent perçue comme contraignante, mais elle permet in fine :

- une homogénéisation des traitements ;
- une amélioration de la qualité globale ;
- une meilleure auditabilité des processus.

QUELS SONT LES PRINCIPAUX DÉFIS LIÉS À UNE IA RESPONSABLE ?

Nos cas d'usage ne relèvent pas de la génération de contenu ou du scoring décisionnel complexe, mais de l'automatisation de contrôles documentaires basés sur des règles auditables.

Nos priorités en matière d'IA responsable concernent principalement :

- la conformité RGPD ;
- la sécurité des données ;
- la capacité à déployer les modèles en local sur notre infrastructure, en particulier pour les banques et assurances ;
- la transparence vis-à-vis des clients sur le fonctionnement des outils, les scores, les seuils et les contrôles.

Nous intégrons des garde-fous à chaque étape du processus afin de garantir que les outils produisent les résultats attendus, sans dérive fonctionnelle ou de confidentialité.

04.

CAS D'USAGES

Finance Innovation

NEXIALOG CONSULTING

PANORAMA DES CAS D'USAGE

Ce cas d'usage présente un benchmark synthétique des pratiques observées dans les grands groupes bancaires et assurantiels.

Les cas d'usage d'IA observés dans les fonctions de contrôle, de gestion des risques et d'audit traduisent une évolution progressive vers des dispositifs de plus en plus intégrés et prédictifs. Le panorama proposé s'organise autour de trois niveaux de déploiement (LoD1 à LoD3), illustrant le passage d'outils d'automatisation documentaire et de détection d'anomalies vers des plateformes d'analyse continue et de scoring prédictif, déployées notamment chez HSBC, ING, BNP Paribas, JPMorgan Chase, Zurich Insurance, KPMG et Wells Fargo, AXA.

PANORAMA DES CAS D'USAGE

LOD1	**HSBC** Détection de fraude et lutte anti-blanchiment	**WELLS FARGO** Scoring et risque de défaut	**JPMORGAN CHASE** Analyse automatisé des contrats
LOD2	**ING** Gestion prédiction du risque de crédit	**ZURICH INSURANCE** Automatisation du contrôle permanent des communications marketing	**AXA** Contrôle permanent de la qualité des souscriptions
LOD3	**BNP** Virtual assistant pour l'Analyse Documentaire, la Synthèse et le Support Conversationnel en Audit	**KMPG CLARA** Audit digitalisé - Automatisation, Analyse Financière, Identification des Risques	**ALLIANZ PARTNERS** Audit digitalisé : Analyses de données avec l'outil CaseWare IDEA

PANORAMA NEXIALOG

CAS D'USAGE	**IA & MODÉLISATION DU RISQUE CYBER** Enrichissement de données pour tarification/provisionnement	**VEILLE RÉGLEMENTAIRE & MAPPING RÉGLEMENTAIRE** Scannings automatisés des évolutions réglementaires, mapping intelligent entre les obligations externes et contrôles internes

04.1. LOD1

AUGMENTÉE : VERS UN CONTROLE OPERATIONNEL INTELLIGENT

La première ligne de défense est la plus exposée aux volumes croissants d'activités de contrôle ainsi qu'à une pression opérationnelle significative et un « business as usual » toujours plus dense. L'IA ouvre la voie à un contrôle interne plus rapide et prédictif. Des cas d'usage tels que la détection d'anomalies de fraudes ou l'automatisation transforment déjà les pratiques.

Ce chapitre explore ce changement avec une réalité terrain, entre gains opérationnels, réallocation des tâches réalisées par l'humain et les nouveaux modes de supervision.

Avant de présenter les cas d'usage, il convient de clarifier les technologies fondamentales de l'IA mobilisées dans le contrôle interne : le Machine Learning (ML), le Natural Language Processing (NLP) et la Robotic Process Automation (RPA).

TECHNOLOGIES IA APPLIQUÉES AU CONTRÔLE INTERNE

MACHINE LEARNING (ML)

Apprentissage automatique à partir des données historiques, amélioration continue sans programmation explicite. Dans le contrôle interne, les modèles gagnent en précision transaction après transaction.

NATURAL LANGUAGE PROCESSING (NLP)

Pour illustrer, 80% des données d'entreprise sont non structurées (contrats, emails, rapports), le NLP transforme ce texte brut en intelligence exploitable : extraction de clauses à risque, analyse de sentiment pour repérer des signaux faibles de non-conformité, synthèse de réglementations massives.

ROBOTIC PROCESS AUTOMATION (RPA)

Automatisation intelligente des contrôles en continu (24/7), couplée à l'IA. Au-delà de la simple automatisation : gestion des exceptions, décisions contextuelles, adaptation aux situations.

L'ETAT DES LIEUX DE LA TRANSFORMATION

L'IA transforme la première ligne de défense en remplaçant les contrôles manuels par une surveillance automatisée en temps réel. Le contrôle devient prédictif plutôt que réactif, permettant aux équipes de se concentrer sur l'analyse stratégique.

Trois domaines sont particulièrement impactés : la fraude et le blanchiment d'argent, le risque de crédit, et le risque de défaut.

Nous illustrons ces propos par des cas d'usage d'IA déjà déployés dans les institutions financières. Les exemples suivants présentent des cas réels d'institutions financières.

L'IA EN ACTION : LES CAS D'USAGES OPÉRATIONNELS

Trois CAS D'USAGE sur les pages qui suivent.

HSBC

CAS D'USAGE DE HSBC : DETECTION DE FRAUDE ET LUTTE ANTI-BLANCHIMENT (AML) : SURVEILLANCE INTELLIGENTE DE 900 MILLIONS DE TRANSACTIONS MENSUELLES

La détection de fraude représente l'un des cas d'usage les plus pertinents de l'IA. Les volumes massifs de transactions, les nombreuses méthodes frauduleuses et le besoin de réactivité en font un domaine idéal pour le machine learning.

CONTEXTE ET DÉFIS

HSBC traite environ 900 millions de transactions chaque mois pour détecter les signes de criminalité financière sur 40 millions de comptes clients. L'approche traditionnelle basée sur des règles fixes générait un taux élevé de faux positifs, mobilisant inutilement les équipes de conformité sur des alertes sans fondement, tout en laissant passer certaines fraudes sophistiquées échappant aux règles prédéfinies.

Le défi était double : améliorer la précision de la détection tout en réduisant la charge de travail manuelle des analystes.

SOLUTION DÉPLOYÉE

HSBC a déployé une architecture d'IA multi-couches combinant plusieurs technologies complémentaires :

- Modèles de machine learning supervisés pour la détection d'anomalies comportementales, apprenant continuellement des patterns historiques de fraude
- Systèmes de surveillance en temps réel intégrant le comportement transactionnel historique de chaque client pour contextualiser les alertes
- NLP (traitement du langage naturel) pour scanner les communications (emails, messages) et documents afin de détecter un langage suspect lié à la fraude ou au blanchiment d'argent
- Plateforme Ayasdi pour l'automatisation et l'optimisation des règles de détection, utilisant la topologie des données pour identifier les clusters de comportements anormaux

BÉNÉFICES OBSERVÉS

- Réduction de 60% des faux positifs/ alertes selon l'équipe conformité de HSBC, permettant aux analystes de se concentrer sur les cas à haut risque
- Diminution des transactions frauduleuses réalisées avec succès en six mois, grâce à une détection plus précoce
- Détection de nouveaux patterns de fraude invisibles aux règles traditionnelles, notamment des schémas de blanchiment multi-étapes sophistiqués
- Gain de temps pour les équipes de conformité, réaffecté à l'analyse des cas complexes

ENSEIGNEMENT CLÉ

L'IA permet de passer d'une approche basée sur des règles rigides à une détection adaptative qui apprend continuellement des nouveaux schémas de fraude.

La combinaison de plusieurs techniques (ML supervisé, NLP, analyse topologique) s'avère plus efficace qu'une approche monolithique.

WELLS FARGO

CAS D'USAGE : GESTION PREDICTIVE DU RISQUE DE DEFAUT (MONITORING CONTINU) WELLS FARGO

Wells Fargo a étendu ses pratiques de modélisation du risque de crédit au-delà de l'octroi initial pour explorer des approches de surveillance continue et d'alerte précoce, en s'appuyant sur des méthodes d'apprentissage automatique explicables afin de concilier performance et conformité.

Wells Fargo : Monitoring et prédiction du risque de défaut en continu.

CONTEXTE ET DÉFIS

Après avoir accordé un crédit, les banques surveillent leurs clients pour repérer les signes de difficultés et intervenir à temps. Wells Fargo a donc mis en place une solution qui détecte les risques de défaut en avance, tout en garantissant deux conditions importantes :

- L'explicabilité des modèles requis par la réglementation
- La réduction des faux positifs entraînant des interventions inappropriées

SOLUTION DÉPLOYÉE

Wells Fargo a recours à une combinaison d'initiatives documentées en interne autour du machine learning explicable et d'un centre d'expertise en analytique quantitative :

- Adaptation des approches XAI (notamment les principes formalisés dans les travaux autour de LIFE – Linear Iterative Feature Embedding) pour rendre interprétables des modèles plus avancés utilisés en monitoring.
- Construction de pipelines de données temps-séries intégrant : données transactionnelles (variations de revenus, découverts, retards de paiement), signaux comportementaux (contacts service client, consultation de solde, changements d'habitudes), et données externes (indicateurs macro-économiques locaux, taux de chômage sectoriel).
- Déploiement d'un système de scoring continu qui génère, pour chaque client, un score de « dégradation de solvabilité » et des explications principales (features contributives) permettant aux équipes de conformité et aux gestionnaires de comptes d'évaluer la pertinence d'une action proactive.
- Gouvernance renforcée : revue régulière des modèles, tests d'équité, suivi de dérive et capacité d'audit pour justifier toute action envers le client (adverse action notice si nécessaire).

BÉNÉFICES OBSERVÉS

- Amélioration de la détection précoce : adoption de modèles ML plus sensibles à de faibles signaux de détérioration, avec la possibilité d'identifier des segments à risque avant que les événements de défaut majeurs n'apparaissent.
- Explicabilité opérationnelle : chaque alerte est accompagnée d'une justification lisible qui facilite l'intervention humaine et la conformité réglementaire.
- Meilleure orchestration des actions client : les équipes de gestion peuvent prioriser les interventions (rééchelonnement, contact proactif) sur la base d'un score et d'un diagnostic clairs.
- Gouvernance & auditabilité : renforcement du suivi des modèles et réduction du risque opérationnel lié aux décisions automatisées.

ENSEIGNEMENT CLÉ

La combinaison d'approches d'IA explicable et d'une gouvernance rigoureuse permet d'envisager un monitoring continu du risque de crédit qui soit à la fois performant et conforme. Cependant, les institutions (dont Wells Fargo) publient rarement des métriques opérationnelles précises publiques (ex. pourcentage exact de défauts anticipés ou économies de pertes), pour des raisons de confidentialité commerciale et réglementaire.

CHASE

CAS D'USAGE : JPMORGAN CHASE COIN (CONTRACT INTELLIGENCE)

Au-delà de la fraude, l'IA transforme également l'analyse des documents contractuels, un domaine où les volumes élevés, la complexité juridique et les contraintes de délai rendent l'automatisation particulièrement pertinente. **JPMorgan Chase : COiN pour l'analyse des documents contractuels**

CONTEXTE ET DÉFIS

JPMorgan Chase devait analyser manuellement de nombreux contrats commerciaux massif par an, un processus mobilisant d'énormes heures de travail juridique. Les risques étaient importants : erreurs d'interprétation, clauses critiques non identifiées, et conséquences opérationnelles et juridiques potentielle.

SOLUTION DÉPLOYÉE

La banque a développé COiN (Contract Intelligence), un système basé sur le NLP et le machine learning capable d'extraire, interpréter et vérifier automatiquement les clauses contractuelles critiques.

BÉNÉFICES OBSERVÉS

- Réduction de 360 000 heures à quelques secondes pour l'analyse d'un contrat type
- Diminution drastique des erreurs d'interprétation manuelle
- Détection automatique des clauses non-standard ou manquantes nécessitant une revue humaine
- Extension progressive à d'autres types de documents (accords de confidentialité, contrats de trading)

ENSEIGNEMENT CLÉ

L'IA excelle dans les tâches répétitives nécessitant une précision absolue. Elle libère les experts pour les cas complexes tout en éliminant les erreurs dues à la fatigue ou à l'inattention.

SYNTHESE – VERS UN CONTROLE CONTINU ET PREDICTIF

Ces trois cas d'usage qu'on vient de voir de la détection de fraude chez HSBC au risque de crédit prédictif de Wells Fargo, en passant par l'automatisation documentaire de JPMorgan schématise le profond changement de la première ligne de défense sous l'effet de l'IA.

Malgré la diversité des champs d'application, des bénéfices convergent :

- Une amélioration spectaculaire de la précision
- Elimination des erreurs manuelles, anticipation des défauts)
- Efficacité économique renforcée
- Rapidité de traitement décuplée (passage de jours à millisecondes).

Les banques basculent désormais vers une surveillance continue 24/7, alimentée par un apprentissage adaptatif capable d'anticiper les risques jusqu'à 6 mois avant leur matérialisation.

Cette évolution redéfinit également les métiers de la LOD1 : les contrôleurs, libérés des tâches répétitives à faible valeur ajoutée, évoluent d'exécutants de processus vers des analystes d'anomalies complexes et des superviseurs d'algorithmes, nécessitant de nouvelles compétences en machine learning, en interprétation de scores IA, et en détection de biais.

Cette montée en expertise, transforme la première ligne de défense en un véritable centre d'intelligence prédictive des risques opérationnels. Toutefois, ces avancées ne doivent pas masquer les limites inhérentes à tout déploiement d'IA ni créer un excès de confiance dangereux.

LIMITES ET PRÉCAUTIONS : L'HUMAIN RESTE INDISPENSABLE

Malgré ces avancées, l'IA ne constitue pas une solution miracle. Plusieurs limites et risques doivent être pris en compte pour éviter un excès de confiance dangereux. La matrice ci-dessous permet d'identifier les principaux risques, d'évaluer leur impact et leur probabilité, de décrire leurs manifestations concrètes et de mettre en place des mesures pour les réduire. Elle précise également les responsables chargés du suivi et les délais de contrôles afin d'assurer une surveillance continue. L'objectif visé est d'encadrer l'usage de l'IA, de structurer sa gouvernance et d'éviter une confiance excessive en garantissant une supervision humaine et organisationnelle.

RISQUE	IMPACT	PROBABILITÉ	MANIFESTATION CONCRÈTE	RECOMMANDATIONS	RESPONSABLE
Faux négatifs	Critique 🔴	Moyenne 🟠	Fraudes sophistiquées non détectées, pertes financières directes	• Équilibre précision/rappel • Supervision humaine transactions >100K€ • Audit mensuel faux négatifs	LOD1 + LOD2
Biais algorithmique	Élevé 🟠	Élevée 🔴	Discrimination clients (géographie, revenus), non-conformité RGPD	• Audits trimestriels fairness • Tests A/B segments • Diversification données entraînement	Data Science + Conformité
Dépendance technologique	Critique 🔴	Faible 🟢	Panne système → incapacité de contrôle, pertes opérationnelles	• Procédures fallback manuelles • 20% processus en mode dégradé • Exercices annuels	IT + LOD1
Explicabilité limitée	Élevé 🟠	Élevée 🔴	Impossibilité justifier décisions, sanctions régulateurs	• Modèles interprétables (SHAP, LIME) • Documentation exhaustive • Formation équipes explicabilité	Data Science
Obsolescence modèles	Modéré 🟢	Élevée 🔴	Baisse performances, fraudes émergentes non détectées	• Réentraînement mensuel • Monitoring continu KPIs • Veille nouveaux patterns	LOD1 + Data Science
Compétences insuffisantes	Élevé 🟠	Moyenne 🟠	Erreurs interprétation, mauvaise utilisation outils	• Formation 40h/an «Contrôleur Augmenté» • Binômes humain-IA • Certification obligatoire	RH + LOD1

Tableau 4.1

CONDITIONS DE SUCCÈS POUR UNE LOD1 AUGMENTÉE PAR L'IA

L'analyse des cas d'usage étudiés met en évidence cinq facteurs de succès, communs à l'ensemble des initiatives ayant démontré une valeur mesurable. Ces facteurs constituent des prérequis opérationnels à toute démarche d'industrialisation de l'IA.

CINQ FACTEURS CLÉS DE SUCCÈS

1 QUALITÉ DES DONNÉES – PRÉREQUIS ABSOLU

- Données fiables, complètes et à jour
- DQI > 85 % requis avant tout modèle
- Gouvernance des données structurée et outillée
  → Sans données de qualité, aucun modèle ne peut performer

2 APPROCHE INCRÉMENTALE ET SÉCURISÉE

- Démarrage par des pilotes ciblés à fort volume
- Validation sur périmètre restreint avant extension
- Montée en charge progressive, sans "big bang"
  → Déploiement maîtrisé, réduction des risques

3 COLLABORATION ÉTROITE MÉTIERS – IT

- Équipes mixtes permanentes (métiers, data, IT)
- Co-construction des modèles et objectifs partagés
- Communication continue tout au long du cycle de vie
  → Modèles alignés avec les enjeux opérationnels

4 SUPERVISION HUMAINE MAINTENUE

- Seuils d'escalade clairement définis
- Processus critiques sous contrôle manuel systématique
- Possibilité d'override et procédures de repli documentées
  → Contrôle humain final et résilience des processus

5 AMÉLIORATION CONTINUE DES MODÈLES

- Réentraînement régulier et monitoring permanent
- Boucles de feedback opérationnelles
- Suivi des KPI en temps réel et veille sur nouveaux risques
  → Performance durable face à des risques évolutifs
- Veille sur nouveaux Patterns

L'IA PERFORMANTE N'EST PAS SEULEMENT UNE QUESTION DE TECHNOLOGIE :

ELLE REPOSE SUR LA DONNÉE, LA GOUVERNANCE, L'HUMAIN ET LA DISCIPLINE OPÉRATIONNELLE

RECOMMANDATIONS STRATÉGIQUES POUR LA LOD1

La LOD1 augmentée par l'IA crée de la valeur uniquement si la technologie est déployée progressivement, portée par des équipes formées et maintenue sous contrôle humain. L'enjeu n'est pas d'automatiser à tout prix, mais de renforcer durablement la performance et la maîtrise des risques.

L'IA représente un levier structurant de performance pour la LOD1, à condition d'être déployée de manière maîtrisée et gouvernée. Les retours d'expérience montrent que la création de valeur ne repose pas sur la technologie seule, mais sur une combinaison équilibrée entre données fiables, compétences humaines et contrôle des décisions.

La priorité stratégique consiste à déployer l'IA de façon progressive, en commençant par des processus à fort volume et à valeur immédiate, tels que la détection de fraude. Cette approche permet de sécuriser les bénéfices, de maîtriser les risques et de préparer l'extension vers des cas plus complexes, sur la base de résultats démontrés. L'objectif à horizon 2027 est une intégration complète de l'IA dans les processus clés de la LOD1.

La réussite de cette trajectoire repose également sur un investissement fort dans les compétences.

L'IA doit renforcer, et non remplacer, l'expertise des équipes. Un programme structurant de formation (« Contrôleur Augmenté ») vise à garantir l'autonomie des collaborateurs et leur capacité à challenger les recommandations des modèles. L'ambition est d'atteindre 100 % des équipes LOD1 formées.

Cette transformation nécessite une architecture technologique évolutive, fondée sur des standards ouverts, une infrastructure cloud scalable et des environnements de test sécurisés, afin d'accompagner la montée en charge et l'innovation continue.

Enfin, le maintien d'un contrôle humain fort sur les décisions critiques constitue un principe non négociable. L'IA doit rester un outil d'aide à la décision, avec des mécanismes d'override et des dispositifs de repli garantissant la résilience opérationnelle.

INTERVIEW

Thomas
VAN MAELE

Cofondateur
et CEO d'Harmoney

Cofondateur et CEO de Harmoney, plateforme RegTech européenne qui automatise et orchestre les workflows de conformité pour les secteurs régulés, il accompagne depuis 2016 plus de 60 assureurs et institutions financières dans la digitalisation de leurs processus de conformité (KYC, KYB, LCB-FT). Son ambition : transformer la contrainte réglementaire en avantage stratégique et faire de la conformité un véritable levier de performance à l'échelle européenne.

« LA CONFORMITÉ N'EST PLUS UN CENTRE DE COÛT : BIEN ORCHESTRÉE PAR L'IA, ELLE DEVIENT UN LEVIER STRATÉGIQUE DE PERFORMANCE ET DE RÉSILIENCE. »

QUELS TYPES DE SOLUTIONS D'IA UTILISEZ-VOUS ET COMMENT AMÉLIORENT-ELLES LE TRAVAIL DES ÉQUIPES ?

Chez Harmoney, nous n'avons jamais cherché à développer un modèle d'IA unique censé tout résoudre. Notre approche consiste à orchestrer plusieurs solutions d'IA déjà existantes sur le marché, et qui sont chacune expertes sur une partie du parcours KYC ou KYB. L'idée, c'est d'utiliser le meilleur outil au bon moment.

Concrètement, cela nous permet d'automatiser la détection de la fraude documentaire, d'améliorer les vérifications d'identité, de faire du screening sur les sanctions ou les PEP, d'identifier les tentatives d'usurpation d'identité et même de mettre automatiquement à jour les données des personnes morales.

Ce que j'observe chez nos clients, c'est que cette approche transforme complètement leur manière de travailler. Les équipes gagnent énormément en efficacité : elles passent moins de temps sur les tâches manuelles, les contrôles sont plus fluides, et la précision s'améliore parce que plusieurs agents d'IA contribuent ensemble au même résultat.

Mais un point reste essential pour nous : l'IA ne décide jamais. Elle assiste, elle accélère, elle fiabilise, mais la décision finale reste humaine. C'est indispensable parce qu'elle doit toujours être explicable face à un auditeur ou un régulateur.

QUELS SONT LES CAS D'USAGE LES PLUS FRÉQUENTS DE VOS CLIENTS ?

Les cas d'usage sont finalement très similaires d'une institution à l'autre. Le premier, c'est l'analyse documentaire automatisée : nos clients veulent identifier plus vite les documents falsifiés ou incohérents, et ils savent que la technologie est désormais très performante sur ce point.

Ensuite, il y a tout ce qui touche à l'identité : vérifier les documents officiels, comparer les photos, détecter les usurpations… Pour un acteur financier, c'est devenu incontournable.

Le screening est aussi très fréquent : l'IA va interroger automatiquement les listes de sanctions, les listes PEP ou encore les sources d'adverse media.

Et pour les personnes morales, nos clients cherchent surtout à reconstituer les organigrammes, les actionnariats ou les liens capitalistiques sans passer des heures à fouiller les registres.

Enfin, il y a la consolidation du risque. C'est quelque chose que je vois beaucoup aujourd'hui : plusieurs agents IA produisent chacun une partie de l'analyse, puis la plateforme orchestre le tout pour obtenir un score de risque global cohérent.

QUELLE EST LA VALEUR AJOUTÉE DE VOTRE PLATEFORME ?

Le premier bénéfice est opérationnel. Les équipes vont plus vite, elles traitent davantage de dossiers et passent moins de temps sur des tâches répétitives. Le parcours KYC ou KYB devient vraiment plus fluide.

Le deuxième bénéfice concerne la qualité du risque. Le simple fait de combiner plusieurs IA permet d'augmenter considérablement le niveau de détection, et également d'assurer une continuité des contrôles. Je pense par exemple aux changements de bénéficiaires effectifs : même si une information évolue, la plateforme assure le suivi automatiquement.

Et puis il y a un point auquel je tiens beaucoup : l'accès continu à la meilleure technologie IA. Intégrer une nouvelle solution peut prendre jusqu'à deux ans dans une banque, alors que la technologie évolue bien plus vite. Avec Harmoney, une institution s'intègre une fois à la plateforme, et nous, de notre côté, faisons entrer la dernière génération de solutions IA sans impact pour elle.

Dans un monde où les fraudeurs innovent aussi vite que les éditeurs d'IA, cette capacité d'adaptation est devenue essentielle.

QUELLES SONT LES LIMITES OU DIFFICULTÉS OBSERVÉES ?

La limite principale, et de très loin, la qualité de la donnée. Si les données ne sont pas à jour dès le départ, tout le reste se dégrade : les modèles d'IA, même les meilleurs, ne peuvent rien faire avec des données incorrectes ou incohérentes. Et aujourd'hui, c'est un problème massif dans les institutions financières.

L'autre difficulté, c'est l'explicabilité. Chaque décision doit pouvoir être justifiée : pourquoi un compte a été bloqué, pourquoi un client a été refusé, etc. C'est pour cela que je maintiens que l'IA ne doit jamais décider seule.

Enfin, il y a le décalage entre la vitesse d'évolution du marché et la lenteur des cycles d'intégration dans les banques. Les fraudeurs se réinventent en permanence, les technologies avancent à grande vitesse, et de l'autre côté, on a des systèmes d'information très lourds et vieillissants, ce qui rend difficile l'intégration rapide de nouvelles briques.

COMMENT VOYEZ-VOUS LES ÉVOLUTIONS DES PROCHAINES ANNÉES ?

Je pense que l'IA va continuer à s'accélérer, et probablement plus vite que ce que l'on imagine aujourd'hui. Les institutions financières devront repenser leur architecture si elles veulent suivre le rythme, et je suis convaincu que les plateformes d'orchestration deviendront la norme.

Mais malgré ces évolutions, je reste convaincu que tout commence par la donnée. Si la qualité de la donnée clients n'est pas solide, l'IA ne pourra jamais donner son plein potentiel.

Finalement, les établissements vont devoir mener deux chantiers en parallèle : améliorer en continu la qualité de la donnée, et rester capables d'intégrer très rapidement les nouvelles technologies. Sans cela, ils seront toujours un train en retard et dans ce domaine, être en retard signifie souvent être vulnérable.

> « DANS LA LUTTE CONTRE LA FRAUDE, ÊTRE EN RETARD TECHNOLOGIQUEMENT REVIENT DÉJÀ À ÊTRE VULNÉRABLE. »

INTERVIEW

Adnane
LAHBABI

Cofondateur
et CTO d'Alphaguard

Alphaguard est une RegTech spécialisée dans la gestion des risques, de la fraude et de la conformité. La solution automatise grâce à des agents IA les tâches chronophages des analystes : lire, croiser et interpréter les données. Alphaguard est aujourd'hui déployée sur des processus LCB-FT, de due diligence, de surveillance continue des tiers et de détection de fraude.

« EN AUTOMATISANT LES CONTRÔLES LES PLUS DÉTERMINISTES, TYPIQUEMENT LE RÉGLEMENTAIRE PUR, ON LIBÈRE LES ANALYSTES POUR LES FAIRE MONTER EN COMPLEXITÉ. »

ALPHAGUARD : D'OÙ VIENT L'IDÉE ?

Avant Alphaguard, j'ai travaillé 5 ans comme Data Scientist chez HP, où je développais des modèles d'IA de détection de fraude. Pour mieux comprendre le travail des investigateurs, je suis devenu CFE (Certified Fraud Examiner), afin de maîtriser les techniques d'investigation au-delà du seul prisme data. Au quotidien, je voyais la même chose se répéter : les systèmes généraient des milliers d'alertes, mais derrière chaque alerte, c'était un investigateur qui devait mener une enquête longue, manuelle, souvent complexe.

Et puis, en novembre 2022, ChatGPT est arrivé avec son potentiel inédit sur l'exploitation des données non structurées. Pour la première fois, on pouvait automatiser ce qui prenait le plus de temps aux analystes : lire, croiser, interpréter. Le potentiel était évident.

C'est à ce moment-là que j'ai quitté HP pour construire la solution qui permettrait à profit cette avancée technologique, et fonder Alphaguard à l'été 2024, avec une conviction simple : on pouvait transformer concrètement la manière dont on lutte contre la fraude et les risques financiers.

POUVEZ-VOUS PARTAGER UN CAS D'USAGE PARTICULIÈREMENT RÉVÉLATEUR ?

Nous travaillons avec une fintech de crédit qui doit, chaque mois, évaluer le risque de l'ensemble de son portefeuille de contreparties. Concrètement, leurs équipes croisaient manuellement des données issues de leurs systèmes internes, d'outils tiers et de recherches internet. Ce travail mobilisait plusieurs jours-homme par mois, principalement sur des tâches répétitives et à faible valeur ajoutée. L'enjeu était double : automatiser ce processus, mais aussi le fiabiliser. Alphaguard a permis de reproduire l'intégralité de ce processus tout en y intégrant de nouvelles sources de données. L'analyse produite est désormais réplicable et entièrement tracée. Surtout, c'est l'orchestration plus fine de l'ensemble de ces données qui a permis de renforcer la détection anticipée des risques en captant des signaux faibles. Les résultats sont tangibles : à périmètre d'équipe constant, la fintech est aujourd'hui en mesure de gérer un portefeuille dix fois plus important, tout en affinant la qualité de l'analyse.

COMMENT L'HUMAIN RESTE-T-IL AU CŒUR DU DISPOSITIF ?

Un point clé de Alphaguard est la boucle d'amélioration continue.

Lorsque l'analyste estime qu'une information ou un commentaire généré par l'IA n'est pas pertinent, ce retour est capturé, intégré et réutilisé pour améliorer les futurs workflows.

Cette collaboration permet de combiner la puissance de l'IA avec l'expertise humaine, plutôt que de les opposer.

TRAVAILLEZ-VOUS SUR D'AUTRES CAS D'USAGE ?

Oui, nous travaillons sur des sujets complexes liés à la fraude qui tirent pleinement parti des capacités des agents IA.

La fraude est par nature un domaine ouvert et non déterministe : les schémas à identifier ne sont pas décrits à l'avance, les signaux faibles sont disséminés dans des volumes importants de données, et les chemins d'investigation sont multiples. C'est précisément là que les agents IA apportent une valeur différenciante : ils sont capables de naviguer dans des environnements complexes, d'explorer des hypothèses multiples et de proposer des pistes d'investigation là où une approche purement règlementaire ou déterministe ne suffit pas.

Concrètement, ces agents peuvent :

- collecter automatiquement les informations pertinentes,
- analyser des documents volumineux,
- identifier des signaux de risque opérationnel,
- proposer des actions de remédiation,
- orchestrer le travail entre agents IA et agents humains.

Certaines tâches chronophages sont déléguées à l'IA, tandis que les décisions critiques restent sous supervision humaine.

COMMENT ABORDEZ-VOUS L'ACCÈS AUX DONNÉES ET LE DÉPLOIEMENT CHEZ LES CLIENTS ?

L'accès aux données est souvent un frein. Alphaguard adopte donc une approche pragmatique en proposant aux clients de démarrer avec des données simulées afin de les mettre en confiance, démontrer rapidement ce qui est faisable, pour accélérer le processus lié à l'accès aux données. Les fintechs disposent de stacks techniques standardisées et nous avons déjà développé les connecteurs adaptés. Les architectures plus complexes demandent un travail d'intégration supplémentaire, que nous intégrons dès le départ dans notre démarche.

QUELS SONT LES OBSTACLES LES PLUS RÉCURRENTS LORS DES DÉPLOIEMENTS ?

Le premier obstacle estde construire une solution crédible pour les métiers.

Notre approche repose d'abord sur la démonstration de la performance. Concrètement, nous travaillons avec les équipes métiers pour ajuster la scorecard de risque, la tester sur des données historiques et démontrer, via du backtesting, les gains qu'Alphaguard aurait permis sur une période donnée, notamment en temps économisé et en qualité d'analyse. Mais, il ne s'agissait pas seulement de démontrer une capacité technologique, mais de s'intégrer aux pratiques existantes.

Pour qu'une solution soit adoptée, elle doit suivre les workflows des équipes métiers, pas l'inverse. C'est pourquoi nous avons une approche très pragmatique, que l'on pourrait qualifier de low touch : simplifier la vie des métiers au maximum. Cela passe par exemple par un niveau fin de notifications adapté à chaque utilisateur, et par la capacité à gérer les actions et le reporting nécessaires directement dans leurs outils existants. L'objectif est que l'IA s'insère naturellement dans le quotidien des équipes, sans friction.

SELON VOUS, QUELS NOUVEAUX RISQUES L'ADOPTION DE L'IA FAIT-ELLE ÉMERGER ?

Le premier enjeu est celui du contrôle des données. Les modèles les plus performants aujourd'hui sont proposés par de grands fournisseurs américains, et les utiliser implique de se poser la question de la maîtrise des données sensibles. Chez Alphaguard, nous avons fait le choix d'une architecture multi-modèles : certains traitements s'appuient sur les modèles les plus performants du marché, tandis que les traitements portant sur des données plus sensibles sont exécutés sur des modèles open source, avec un contrôle strict de la donnée, notamment au sein d'infrastructures souveraines. Cette approche nous permet de combiner performance et maîtrise, sans compromis.

Le second risque souvent évoqué est celui de la perte d'expertise métier. Certains analystes craignent de devenir de simples validateurs des décisions de l'IA. Ma conviction est inverse : l'IA doit donner plus de sens au métier. En automatisant les contrôles les plus déterministes, typiquement le réglementaire pur, on libère les analystes pour les faire monter en complexité, vers des analyses de fraude complexe assistée par l'IA, là où leur expertise a le plus de valeur. L'IA ne remplace pas le métier, elle le déplace vers le haut.

QUELS CAS D'USAGE IA VOUS SEMBLENT LES PLUS PROMETTEURS À COURT/MOYEN TERME ?

Les contraintes réglementaires vont mécaniquement imposer davantage de contrôles. Les acteurs soumis à ces exigences auront besoin de solutions capables d'automatiser, de tracer, et d'expliquer la donnée.

Mais le potentiel le plus fort reste selon nous la fraude, car elle est par nature moins prédictible que le réglementaire. Contrairement aux contrôles normés, la fraude évolue en permanence, avec des schémas complexes et contextuels.

Chez Alphaguard, nous analysons des environnements complexes où la densité de mouvements et la variété des signaux permettent de détecter des risques qu'aucun système déterministe ne pourrait anticiper seul.

04.2. LOD2

A L'ÈRE DE L'IA : RISQUES & CONFORMITÉ EN PLEINE MUTATION

LE RÔLE FONDAMENTAL DE LA 2e LIGNE DE DÉFENSE

Dans le modèle international des Trois lignes de défense (Institute of Internal Auditors, 2020), la 2e ligne de défense (LOD2) regroupe les fonctions de gestion des risques, conformité et contrôle permanent. Son rôle est d'établir les politiques, de superviser la 1re ligne (les métiers opérationnels) et de fournir une vision indépendante des risques à la gouvernance.

Elle ne se substitue pas à l'audit interne (3e ligne), mais garantit la cohérence, la traçabilité et l'exhaustivité du dispositif global de maîtrise des risques.

L'IMPACT DE L'INTELLIGENCE ARTIFICIELLE :

L'essor de l'IA transforme profondément les fonctions Risques & Conformité.

Elle amplifie le potentiel d'analyse, mais crée aussi des risques nouveaux : opacité algorithmique, biais de données, dérive de modèle, responsabilité juridique, sécurité et conformité éthique.

LA LOD2 RÉINVENTÉE : NOUVEAUX PILIERS DE GOUVERNANCE

La LOD2 évolue d'une fonction de surveillance périodique et rétrospective vers un rôle de pilotage continu et prédictif.

Cette transformation ne se limite pas à automatiser les contrôles de conformité existants. Elle anticipe surtout les risques émergents et adapte les stratégies de mitigation en fonction de l'évolution de l'environnement réglementaire.

L'IA transforme les équipes Risk & Compliance en véritables centres d'intelligence stratégique, capables de traiter des volumes massifs d'informations pour en extraire des recommandations actionnables.

Cette évolution redéfinit le rôle des professionnels du risque, qui deviennent des analystes prédictifs, plutôt que de simples contrôleurs a posteriori.

Face à ces mutations, les équipes LOD2 évoluent autour de trois axes structurants.

LES TROIS NOUVEAUX PILIERS DE LA LOD2.

GOUVERNANCE ET CADRE MÉTHODOLOGIQUE DE L'IA

La LOD2 définit désormais :

- une stratégie IA alignée sur l'appétence au risque ;
- des politiques de gouvernance des données et des modèles ;
- des critères d'éthique, d'équité et d'explicabilité applicables aux systèmes IA.

Elle évalue la robustesse des modèles, documente les risques de biais, et met en place des procédures de validation, de stress-testing et de revue indépendante.

SUPERVISION ET CHALLENGE OPÉRATIONNEL

La LOD2 assure un contrôle continu des usages IA par la 1re ligne :

- suivi de la performance et des dérives de modèles (KRI IA) ;
- vérification des mesures de mitigation des risques IA ;
- audit interne des pipelines de données et des décisions automatisées.

Elle agit en partenaire critique des métiers et de l'IT, garantissant que les solutions IA respectent les politiques internes et réglementaires.

TRANSPARENCE ET AMÉLIORATION CONTINUE

La LOD2 devient aussi un acteur de la pédagogie IA :

- diffusion d'une culture de la conformité algorithmique ;
- reporting régulier sur les incidents IA et la performance des contrôles ;
- adaptation constante aux évolutions réglementaires (IA Act, DORA, RGPD).

ÉVOLUTION DU RÔLE DE LA LOD2

L'IA permet à la LOD2 de passer d'un contrôle a posteriori à une supervision continue et anticipative, renforçant la maîtrise des risques et la qualité du pilotage stratégique.

L'introduction de l'IA transforme en profondeur le rôle de la LOD2, qui évolue d'une logique de contrôle périodique et rétrospectif vers une supervision continue, anticipative et stratégique. Cette évolution ne remet pas en cause les missions fondamentales de la LOD2, mais en renforce significativement l'efficacité, la portée et la valeur ajoutée.

Avant l'IA, les dispositifs de LOD2 reposaient principalement sur des analyses a posteriori, des contrôles manuels réalisés par échantillonnage et une capacité limitée à traiter de grands volumes de données.

Avec l'IA, la LOD2 accède à un pilotage en temps réel des risques, fondé sur l'analyse automatisée et exhaustive des données, permettant d'identifier plus tôt les dérives, les signaux faibles et les zones de fragilité du dispositif de contrôle interne.

Concrètement, plusieurs cas d'usage IA structurants illustrent cette transformation. L'IA permet, par exemple, un monitoring continu des indicateurs de risque et de conformité, avec détection automatique des anomalies et des ruptures de tendance. Elle facilite également l'analyse prédictive des risques émergents, en anticipant l'apparition de schémas atypiques ou de comportements à risque.

Dans le cadre du contrôle de la LOD1, l'IA renforce la capacité de la LOD2 à réaliser des revues exhaustives et ciblées, en orientant les contrôles vers les zones à risque, plutôt que vers des échantillons limités. Enfin, l'exploitation de volumes de données massifs permet de produire des analyses transverses et comparatives, utiles au pilotage global des risques et à l'éclairage des décisions de gouvernance.

Cette évolution repositionne la LOD2 dans un rôle d'analyste stratégique, capable d'interpréter les résultats des modèles, de challenger les dispositifs existants et d'apporter une vision prospective aux instances dirigeantes.

AFIN DE BIEN CONSTATER CES ÉVOLUTIONS, NOUS VOUS PROPOSONS QUELQUES CAS D'USAGE DE MODÈLE D'IA DÉPLOYÉ SUR LA LOD2.

ING

CAS D'USAGE ING : LA GESTION PREDICTIVE DU RISQUE DE CREDIT

Dans un contexte réglementaire caractérisé par des exigences accrues de rapidité d'analyse, ING figure parmi les acteurs européens ayant intégré l'intelligence artificielle dans la gestion du risque de crédit.

CONTEXTE ET DÉFIS

- L'objectif : améliorer la détection précoce des signaux de détérioration, renforcer la qualité des décisions et accroître l'efficacité des processus.
- Le scoring en temps réel avec l'outil "CheckAhead".

SOLUTION DÉPLOYÉE

AUTOMATISATION DU PROCESSUS DE CRÉDIT

ING a développé des solutions basées sur l'analyse avancée des données et le machine learning pour soutenir l'évaluation du risque de crédit. Selon ING, ces outils permettent de surveiller des données financières et non financières, d'identifier des anomalies et de détecter plus tôt les signes de dégradation du risque.
La filiale ING Real Estate Finance a également déployé, avec le cabinet IG&H, un dispositif d'automatisation des revues de crédit reposant sur la modélisation et l'analyse algorithmique. Ce dispositif a permis :

- D'automatiser environ 80 % des revues de crédit,
- D'automatiser environ 50 % des extensions de prêts.

BÉNÉFICES OBSERVÉS

Selon les retours publiés par ING et IG&H, l'automatisation et l'analyse avancée ont permis :

- D'accélérer le traitement des dossiers,
- D'augmenter le volume de revues sans mobilisation de ressources supplémentaires,
- De renforcer la traçabilité et la qualité des décisions de crédit.

ENSEIGNEMENT CLÉ

ING Group a fait de l'IA un accélérateur de performance dans la gestion du risque de crédit, avec une logique claire : détecter les problèmes avant qu'ils ne coûtent cher. Le dispositif repose sur trois leviers opérationnels. D'abord, l'anticipation : l'IA analyse en continu des milliers de signaux pour repérer les premiers signes de fragilité financière des emprunteurs, transformant la banque d'un acteur réactif en acteur prédictif. Ensuite, l'automatisation : les revues de crédit routinières sont traitées par la machine, multipliant la capacité de surveillance sans alourdir les coûts. Enfin, la gouvernance : toute décision sensible – accord, refus, restructuration – reste sous contrôle humain, garantissant responsabilité et conformité réglementaire.

Ce modèle hybride démontre que l'IA n'est pas un substitut mais un amplificateur : elle excelle dans le traitement massif de données, l'humain conserve le jugement stratégique. L'avantage compétitif ne vient pas de la technologie seule, mais de son déploiement maîtrisé : progressif pour limiter les risques, transparent pour assurer l'acceptabilité, conforme pour sécuriser l'exploitation. ING illustre ainsi qu'en matière bancaire, l'innovation rentable est celle qui optimise le binôme efficacité-prudence.

ZURICH

ZURICH INSURANCE – AUTOMATISATION DU CONTROLE PERMANENT DES COMMUNICATIONS MARKETING

Avec la multiplication des canaux digitaux (sites web, réseaux sociaux, campagnes marketing, publicités en ligne, supports digitaux variés), les entreprises et plus particulièrement les acteurs fortement réglementés comme les assureurs font face à un défi croissant : comment garantir, en continu, la conformité des contenus diffusés ?

CONTEXTE ET DÉFIS

Le volume, la fréquence et la diversité des communications rendent une relecture manuelle exhaustive impraticable : outre le coût et le temps, le risque d'erreurs humaines augmente. Par ailleurs, les exigences réglementaires (transparence, non-tromperie, évitement du "greenwashing", respect des promesses faites aux consommateurs…) poussent à un contrôle rigoureux, homogène et traçable.

Dans ce contexte, l'émergence des technologies d'intelligence artificielle offre une opportunité : automatiser la détection de non-conformités, standardiser les vérifications et permettre une surveillance permanente, tout en libérant les équipes de conformité des revus systématiques.

SOLUTIONS DÉPLOYÉES

Zurich a intégré une solution Haast pour automatiser la revue de ces contenus afin de garantir la conformité des communications marketing (documents, sites, réseaux sociaux…)

L'outil déployé devra permettre :

- Analyse automatisée des contenus
- Surveillance continue et automatisée des canaux numériques
- Intégration de workflows existants
- Tableau de bord centralisé

BÉNÉFICES OBSERVÉS

L'intégration d'une solution d'IA dédiée au contrôle des communications marketing répond à plusieurs ambitions clés :

- Accroître l'efficacité opérationnelle : automatiser la revue de supports afin de réduire la charge humaine et fluidifier les processus de validation.
- Prioriser les risques : identifier les contenus présentant un risque de non-conformité afin que LOD2 concentre ses efforts sur les cas critiques et à forte exposition.
- Sécuriser les communications : détecter en amont les écarts réglementaires, les formulations trompeuses ou les messages sensibles, tout en garantissant une homogénéité des contrôles.
- Améliorer la traçabilité : conserver les analyses, alertes et arbitrages dans un référentiel unique, facilitant le reporting, l'audit et la justification auprès des régulateurs.
- Permettre une surveillance continue : assurer un monitoring digital 24/7 et une capacité de réaction rapide en cas de dérive.

L'IA devient un outil d'aide à la décision, permettant de gagner en rigueur, en couverture et en rapidité d'analyse.

ENSEIGNEMENT CLÉ

L'IA constitue un levier de maturité pour la ligne de défense 2 : elle fluidifie l'analyse, fiabilise l'identification des risques et permet une couverture de contrôle plus large, plus homogène et plus continue. Elle s'inscrit dans une logique d'industrialisation du dispositif de conformité, tout en renforçant la capacité de pilotage, de reporting et de preuve.

Son efficacité dépend cependant de la qualité du paramétrage, d'une supervision experte et d'un modèle de gouvernance solide. Placée comme un outil au service de la conformité, et non comme un substitut décisionnel, elle permet à LOD2 d'augmenter sa performance, sa valeur ajoutée et son rôle stratégique dans la maîtrise des risques de communication.

AXA

CAS D'USAGE : AXA

Dans le secteur de l'assurance, la qualité de la souscription détermine directement la rentabilité des portefeuilles.

CONTEXTE ET DÉFIS

AXA contrôle la conformité de milliers de contrats émis quotidiennement par ses réseaux d'agences et de courtiers.

Les méthodes traditionnelles d'audit par échantillonnage (5-10% des contrats) laissaient passer des acceptations hors normes : tarifs incorrects, garanties inadaptées au profil de risque, ou surprimes insuffisantes. Ces dérives impactaient la rentabilité technique et créaient des disparités entre agences.

SOLUTIONS DÉPLOYÉES

AXA a déployé un système d'analyse automatisée des décisions de souscription basé sur le machine learning :

- Machine Learning supervisé : Algorithmes entraînés sur l'historique des souscriptions pour identifier les patterns de non-conformité
- Moteur de règles avancé : Vérification automatique de centaines de critères de conformité technique
- Dashboards analytics : Visualisation des tendances de qualité par souscripteur, agence, produit et région

BÉNÉFICES OBSERVÉS

- **Intégration temps réel :** Connexion directe aux systèmes de souscription pour analyse immédiate lors de l'émission
- **Contrôle exhaustif en temps réel :** Analyse de 100% des contrats dès leur création (vs échantillonnage manuel limité)
- **Scoring de qualité automatique :** Chaque souscription reçoit un score de conformité basé sur les politiques techniques (tarification, limites de garanties, profils acceptables)
- **Alertes ciblées :** Détection immédiate des écarts aux politiques et notification automatique au souscripteur pour correction avant validation définitive
- **Analyses prédictive :** Identification des patterns de dérive par souscripteur, agence ou type de produit, permettant des actions préventives (formation, ajustement des délégations)
- Réduction de 35% des contrats hors normes acceptés (surprimes insuffisantes, garanties non conformes, limites dépassées)
- **Détection précoce des dérives :** Identification immédiate des écarts aux politiques de souscription avant validation définitive
- **Harmonisation des pratiques :** Standardisation des décisions entre agences et réduction des disparités de qualité
- **Amélioration de la rentabilité technique :** Meilleure adéquation tarif/risque sur l'ensemble du portefeuille
- **Optimisation des contrôles humains :** Concentration des revues manuelles sur les cas complexes identifiés par l'IA

ENSEIGNEMENT CLÉ

L'IA permet de passer d'un contrôle par échantillonnage a posteriori à une surveillance exhaustive en temps réel. Ce changement de paradigme transforme le rôle de la LOD2 : d'une fonction de détection rétrospective, elle devient un dispositif de prévention proactive, guidant les opérationnels vers des décisions conformes avant même leur finalisation. La clé du succès réside dans l'équilibre entre automatisation (exhaustivité, rapidité) et expertise humaine (cas complexes, ajustement des politiques).

SYNTHÈSE DE CAS D'USAGE : L'IA AU SERVICE DE LA GESTION DES RISQUES ET DE LA CONFORMITÉ

Les initiatives de ING Group, Zurich Insurance Group et AXA mettent en évidence une transformation profonde des fonctions de gestion des risques et de conformité grâce à l'IA. Malgré leurs activités distinctes, ces trois entreprises utilisent l'IA de façon similaire pour améliorer leurs contrôles internes et conformité.

A travers ces cas d'usage, ING accélère l'évaluation du risque de crédit et automatise les revues, AXA contrôle l'intégralité des décisions de souscription dès leur émission, et Zurich assure un monitoring continu de ses communications marketing.

Au-delà de l'efficacité, l'IA contribue également à standardiser l'application des règles, à réduire les disparités de pratiques et à améliorer la traçabilité des contrôles. Elle devient ainsi un outil structurant pour les fonctions de contrôle permanent, facilitant le reporting, l'auditabilité et la justification auprès des régulateurs. Dans tous les cas étudiés, l'IA n'a pas vocation à remplacer les équipes de contrôle, mais bien à augmenter leur portée, leur rigueur et leur capacité de pilotage.

Ces bénéfices s'accompagnent toutefois de limites et d'exigences clairement identifiées. La supervision humaine demeure indispensable pour valider les décisions sensibles et interpréter correctement les alertes générées. Les risques de faux positifs, de faux négatifs et de biais algorithmiques imposent un cadre de gouvernance solide intégrant auditabilité, explicabilité des modèles et revues régulières. La performance des solutions dépend par ailleurs étroitement de la qualité des données, du paramétrage initial et de la mise à jour continue des règles. L'enrichissement des données externes et la transparence accrue des modèles constituent des enjeux majeurs pour les évolutions futures.

En définitive, l'IA représente un levier stratégique de transformation des fonctions risques et conformité, à condition d'être déployée comme un outil d'aide à la décision, intégré dans un dispositif gouverné, progressif et centré sur l'expertise humaine. Bien maîtrisée, l'IA ne se limite pas à optimiser les processus existants : elle fait évoluer fondamentalement la posture des fonctions de contrôle, d'une logique de détection rétrospective vers une approche proactive, préventive et créatrice de valeur.

LES DÉFIS MAJEURS DE LA LOD 2 À L'ÈRE DE L'IA

CONSTATS	DESCRIPTIONS
Compétences techniques	Développer une compréhension des modèles IA et de la data science pour challenger efficacement la 1re ligne.
Gouvernance des données	Garantir la qualité, la traçabilité et la conformité des jeux de données utilisés.
Explicabilité et transparence	S'assurer que chaque modèle est documenté et interprétable, même pour des non-experts.
Culture collaborative	Coopérer étroitement avec les équipes data, IT et métiers pour assurer un contrôle « by design ».
Évolution réglementaire rapide	Adapter en continu les dispositifs internes aux exigences du futur cadre européen de l'IA.

Tableau 4.2

RECOMMANDATIONS STRATÉGIQUES POUR LA LOD2

GOUVERNANCE RENFORCÉE DE L'IA

L'ampleur de la transformation nécessite une gouvernance adaptée au plus haut niveau de l'organisation. La création d'un AI Risk Committee au niveau du Conseil d'Administration signale l'importance stratégique accordée à ces enjeux et garantit l'allocation des ressources nécessaires. Un framework de validation des modèles avec trois niveaux de criticité (faible, modéré, élevé) permet de dimensionner les contrôles en fonction des enjeux. La revue trimestrielle de tous les modèles en production assure un suivi continu de leurs performances et de leur conformité. Enfin, un RACI spécifique pour les décisions algorithmiques clarifie les responsabilités et évite les zones grises préjudiciables à la gouvernance.

CONFORMITÉ BY DESIGN

L'approche traditionnelle qui consiste à adapter les systèmes aux exigences réglementaire a posteriori doit être remplacée par une méthode de *« conformité intégrée dès la conception »*

PRINCIPE	MISE EN ŒUVRE
Intégration réglementaire dès la conception	Checklist IA Act obligatoire en phase de design
Documentation automatique	Génération automatique de piste d'audit
Tests systématiques	Batterie de tests robustesse + biais avant déploiement
FRIA systématique	Évaluation d'impact sur les droits fondamentaux

Tableau 4.3

LES BÉNÉFICES DE CETTE APPROCHE

- Évite des refontes coûteuses et tardives
- Accélère le processus de conformité
- Diminue les risques réglementaires
- Facilite la réalisation d'audits internes et externes

MONTÉE EN COMPÉTENCES

La transformation des métiers nécessite un effort de formation sans précédent. Une formation obligatoire en data science pour l'ensemble des collaborateurs de la LoD2 est important pour se mettre à niveau vis à vis de l'attendu côté maitrise des nouveaux outils. Le recrutement de profils hybrides permet aussi d'enrichir les équipes avec de nouvelles expertises. Les collaborations avec des universités facilitent le développement de programmes de formation sur mesure. La certification des utilisateurs clés sur les outils d'intelligence artificielle assure leur maîtrise opérationnelle.

INTERVIEW

Anthony
LEVEL

LABEL4.AI

Co-fondateur et Chief Strategy Officer de Label4.ai

Spécialiste des enjeux de confiance numérique et de régulation de l'intelligence artificielle, il pilote la stratégie institutionnelle et les partenariats stratégiques de l'entreprise. Il intervient régulièrement sur les sujets de traçabilité et de détection des contenus générés par IA, en lien avec les acteurs publics et les secteurs régulés. Il contribue notamment aux travaux relatifs à la transparence des contenus IA auprès de la Commission européenne.

« À L'ÈRE DES CONTENUS SYNTHÉTIQUES INDISCERNABLES, LA DÉTECTION DE L'IA DEVIENT UNE LIGNE DE DÉFENSE STRATÉGIQUE POUR PRÉSERVER LA CONFIANCE ET MAÎTRISER LE RISQUE. »

PRÉSENTATION DE LA TECHNOLOGIE

Label4.ai est une deeptech souveraine issue des laboratoires de recherche publics Inria et CNRS, qui développe des solutions à la pointe de détection et de traçabilité des contenus générés ou manipulés par intelligence artificielle, spécifiquement adaptées aux environnements à forte contrainte réglementaire comme la banque et l'assurance. En ayant la capacité de reconnaitre les contenus synthétiques, Label4.ai peut neutraliser les deepfakes avant qu'ils aient un impact négatif sur les organisations.

DÉTECTER L'IA POUR PRÉSERVER LA CONFIANCE NUMÉRIQUE

L'essor de l'IA générative fait émerger un enjeu critique : la capacité des organisations à distinguer le vrai du faux dans des contenus toujours plus réalistes. Images, documents, audio ou vidéo manipulés peuvent désormais être produits à grande échelle, exposant les entreprises à de nouveaux risques de fraude, d'usurpation et de manipulation documentaire.

Dans ce contexte, Label4.ia, startup deep tech française en collaboration avec le CNRS et l'INRIA,

développe des solutions dédiées à la détection de contenus générés ou altérés par IA. L'objectif est de sécuriser les processus sensibles : vérification d'identité, gestion documentaire, traitement des sinistres, audit ou prévention des fraudes vocales et visuelles alors que de nombreux secteurs restent encore insuffisamment équipés face à ces nouvelles menaces.

La technologie repose sur une combinaison d'analyses : métadonnées, anomalies sémantiques, signatures invisibles des modèles génératifs et tatouages numériques. Cette approche multi-couches permet une détection rapide et explicable, adaptée aux exigences des fonctions de contrôle, de risque et de conformité.

À mesure que les modèles génératifs gagnent en réalisme, la détection des contenus synthétiques s'impose comme un levier essentiel pour sécuriser les opérations, renforcer la confiance numérique et anticiper les nouveaux cadres réglementaires liés à l'IA.

CAS D'USAGE AUJOURD'HUI LES PLUS DEMANDÉS

Dans les secteurs banque et assurance, les demandes les plus fréquentes concernent :

- la fraude documentaire augmentée par IA (RIB générés, faux justificatifs de domicile, déclarations de sinistres manipulés...)
- les deepfakes vidéo et vocaux relatifs à l'usurpation d'identité (faux dirigeant demandant un virement, faux assuré déclarant un sinistre, contournement des KYC et onboarding...)
- les sinistres et déclarations manipulés (Images de dommages générées ou amplifiées par IA, vidéos manipulées dans des dossiers contentieux...)

UN CAS D'USAGE RÉEL PARTICULIÈREMENT RÉVÉLATEUR

Un assureur a été confronté à une série de déclarations de sinistres automobiles accompagnées de photographies de dommages générées ou amplifiées par IA. À l'œil humain, les images étaient cohérentes : ombres crédibles, cohérence géométrique apparente, métadonnées plausibles.

L'analyse forensic Label4.ai a permis d'identifier : des incohérences fréquentielles invisibles à l'œil nu, des motifs statistiques typiques des modèles génératifs ainsi qu'une homogénéité anormale dans les textures. Les dossiers ont été réévalués avant indemnisation.

S'équiper d'un outil de détection d'IA permet de réduire les indemnisations frauduleuses qui ne sont pas détectées aujourd'hui.

En assurance automobile, une fraude moyenne sur sinistre automobile peut représenter en moyenne entre 2 000 € et 15 000 € selon le dossier.

Quelques dizaines de dossiers détectés représentent rapidement plusieurs centaines de milliers d'euros évités. Une réduction marginale de 0,5 à 1 point du ratio sinistres/primes peut avoir un impact direct significatif sur la rentabilité d'un portefeuille.

Ceci permet également une optimisation des ressources humaines (moins d'enquêtes inutiles, meilleur ciblage des dossiers suspects, réduction du temps d'analyse par dossier, la détection automatisée permet de concentrer l'expertise humaine sur les cas réellement complexes).

En identifiant rapidement les contenus non manipulés, l'assureur peut dans le même temps : accélérer l'indemnisation des clients honnêtes, améliorer la satisfaction client et réduire le risque réputationnel.

LA PLACE DE LA DÉTECTION / TRAÇABILITÉ IA DANS LES DISPOSITIFS DE CONTRÔLE À VENIR

Dans la banque et l'assurance, la détection IA va devenir une nouvelle ligne de défense structurante. Elle s'intègrera comme extension des contrôles KYC / souscription, comme brique complémentaire des moteurs anti-fraude traditionnels, comme outil d'investigation post-sinistre et comme élément de cartographie du risque technologique.

À moyen terme, elle devrait figurer dans les référentiels de contrôle interne et dans les dispositifs de gestion du risque opérationnel.

LES USAGES CLÉS QUI, SELON VOUS, VONT SE DÉVELOPPER D'ICI 2030

La fraude augmentée par IA va se démocratiser. La capacité à distinguer un contenu authentique d'un contenu synthétique deviendra un standard de maîtrise du risque dans les secteurs banque et assurance. D'ici 2030, nous anticipons un contrôle systématique des pièces justificatives via détection d'intervention d'IA, une détection temps réel dans les interactions téléphoniques, visios et centres d'appel (détection de voix synthétique), une certification des documents contractuels émis par l'assureur ainsi qu'une intégration des signaux IA dans les modèles de scoring fraude.

04.3. LOD3

L'AUDIT DU FUTUR : COMMENT L'IA TRANSFORME LA 3e LIGNE DE DEFENSE

L'AUDIT CONTINU COMME NOUVEAU PARADIGME

La troisième ligne de défense connaît peut-être la transformation la plus radicale de toutes. L'audit périodique conventionnel annuel ou trimestriel cède la place à un audit continu, prédictif et prescriptif. Cette évolution soutient non seulement l'accélération des processus actuels, mais aussi des scénarios simulés de risque avant qu'ils ne se produisent, transformant l'audit d'une simple fonction de contrôle rétrospective en un outil proactif et utile pour le processus de planification et de prise de décision. Ce changement fondamental repositionne la fonction d'audit, non plus comme un outil de contrôle, mais plutôt comme un partenaire stratégique de la direction, capable d'offrir une analyse prédictive sur les faiblesses et les améliorations à apporter. Avec l'IA, ils peuvent digérer d'énormes quantités de données impossibles à traiter manuellement, découvrant des corrélations et des anomalies sans doute cachés à l'œil humain.

BNP

BNP PARIBAS : VIRTUAL ASSISTANT DE L'INSPECTION GÉNÉRALE (2024)

CONTEXTE ET DÉFIS

Au sein de l'Inspection Générale de BNP Paribas, l'analyse des documents d'audit représentait un défi majeur où les volumes étaient élevés, et les exigences de confidentialité particulièrement critiques. Les auditeurs devaient traiter manuellement d'importants volumes de documentation, un processus mobilisant d'énormes heures de travail analytique.

LES RISQUES ÉTAIENT IMPORTANTS

Erreurs d'interprétation manuelle clauses manquantes ou mal identifiées, et conséquences opérationnelles et de conformité potentielles.

La nécessité d'une solution permettant de moderniser les processus d'audit tout en garantissant la souveraineté et la sécurité des données sensibles était devenue incontournable.

SOLUTION DÉPLOYÉE

L'assistant basé sur l'IA générative, déployé au sein de l'Inspection Générale de BNP Paribas, fait partie de la plateforme interne de BNP Paribas « Large Language Model – LLM as a Service ». Afin d'analyser les documents et de moderniser les processus d'audit tout en maintenant la confidentialité des données .

BÉNÉFICES OBSERVÉS

- Gain de temps et efficacité analytique : les auditeurs disposent d'un outil capable de traiter rapidement de grands volumes de documentation, facilitant la préparation des missions et la rédaction de synthèses.
- Amélioration de la recherche documentaire : l'assistant permet de poser des questions en langage naturel sur des corpus internes, ce qui fluidifie l'accès à l'information.
- Sécurité et souveraineté des données : l'usage d'un LLM hébergé sur les infrastructures internes de BNP Paribas (et non sur des services publics comme ChatGPT) garantit la confidentialité des données sensibles de l'audit.
- Acculturation à l'IA générative : le projet s'inscrit dans une stratégie plus large de montée en compétence des collaborateurs et d'intégration responsable des technologies IA au sein du groupe.

ENSEIGNEMENT CLÉ

- L'IA excelle dans les tâches répétitives : elle libère les auditeurs de l'analyse de volumes massifs pour se concentrer sur le jugement à forte valeur ajoutée
- La qualité des données conditionne la fiabilité : des documents incomplets ou mal structurés produisent des analyses biaisées ou inexactes
- L'humain reste indispensable : la supervision et la validation par les experts demeurent cruciales, l'IA assiste mais ne décide pas
- La souveraineté des données est non négociable : l'hébergement interne s'impose pour garantir confidentialité et conformité réglementaire
- L'adoption est progressive : expérimentation, ajustements itératifs et accompagnement au changement sont aussi importants que la technologie
- La gouvernance encadre l'usage : chartes internes, processus de validation et contrôles éthiques sont les gardes-fous d'un déploiement responsable

Ce travail sur les assistants virtuels de l'inspection générale a été l'un des premiers exemples d'utilisation directe de l'intelligence générative dans le fonctionnement interne d'une organisation d'un grand groupe bancaire européen. Cette initiative souligne l'aspiration de la banque à infuser des technologies souveraines et sécurisées avec une gouvernance humaine robuste. Les premiers retours suggèrent qu'il est nettement plus efficace et fournit des outils d'analyse améliorés pour les auditeurs, bien que l'adoption, la fiabilité et l'éthique de ces solutions restent un défi.

KPMG

KPMG :
INTÉGRATION DE L'IA GÉNÉRATIVE DANS KPMG CLARA

CONTEXTE ET DÉFIS

KPMG fait face aux défis classiques de l'audit : volume croissant de données à analyser, tâches répétitives chronophages, pression sur les délais et nécessité d'améliorer la détection des risques. La profession d'audit nécessite rigueur et exhaustivité, mais les méthodes traditionnelles atteignent leurs limites face à la complexité et au volume des données financières modernes.

SOLUTION DÉPLOYÉE

Dès 2024, KPMG a intégré l'IA générative dans sa plateforme d'audit KPMG Clara, avec le soutien de Microsoft (Copilot) et des plateformes transverses (Digital Gateway Gen AI, KPMG Velocity), pour moderniser d'audit et renforcer l'efficacité des équipes tout en maintenant la supervision humaine (« human in the loop »).
C'est une plateforme d'audit intelligente qui automatise les tâches répétitives, analyse les données financières en continu et fournit aux auditeurs des insights plus profonds pour améliorer la qualité et la rapidité des audits.

BÉNÉFICES OBSERVÉS

- Automatisation des tâches et gain de temps
- Analyse des rapports financiers
- Détection des anomalies et des risques
- Soutien méthodologique et acculturation à l'IA à travers le portail collaboratif
- Extension à d'autres métiers pour un alignement global

ENSEIGNEMENT CLÉ

- L'IA générative est un multiplicateur de capacités, pas un substitut : elle augmente l'expertise humaine mais ne remplace pas le jugement professionnel de l'auditeur
- La supervision humaine reste indispensable : les risques d'hallucinations, de biais et d'erreurs de l'IA générative exigent un contrôle systématique
- La qualité des données conditionne la performance : l'efficacité de l'IA dépend directement de la fiabilité et de la structuration des données sources
- Le déploiement doit être progressif et localisé : adaptation aux spécificités réglementaires et métiers de chaque marché, avec une conduite du changement rigoureuse
- La transformation est autant organisationnelle que technologique : nécessité de repenser les processus, former massivement les équipes et établir une gouvernance stricte
- La mesure des impacts reste un défi : évaluation continue du ROI et de l'efficacité réelle nécessaire pour piloter la transformation et justifier les investissements

Mais il convient de rester attentif aux conditions de mise en œuvre : gouvernance, qualité des données, supervision humaine, adaptation locale et mesure précise des impacts restent des défis à relever.

ALLIANZ

ALLIANZ PARTNERS & L'INTÉGRATION DE L'ANALYSE DE DONNÉES DANS L'AUDIT INTERNE

CONTEXTE ET DÉFIS

Allianz Partners, spécialisée en assurance assistance, a modernisé son audit interne grâce à l'analyse de données. Face aux volumes importants de transactions, sinistres et données clients, son l'objectif était d'améliorer la qualité, la fiabilité et la rapidité des contrôles.

SOLUTION DÉPLOYÉE

La solution repose sur CaseWare IDEA, une plateforme d'audit analytics qui analyse de grands volumes de données (sinistres, primes, transactions) pour détecter automatiquement les anomalies, erreurs et comportements suspects. Les équipes d'audit collaborent étroitement avec des experts en data analytics et le partenaire technologique pour :

- normaliser les données sources ;
- transformer des questions d'audit en tests analytiques automatisés ;
- intégrer ces tests dans un cadre structuré d'analyse intégré au workflow d'audit.

Allianz Partners a créé des applications spécifiques autour d'IDEA pour différents domaines d'audit (notamment Claims & Assistance), intégrant des tests ciblés comme :

- vérification de la justification des sinistres par rapport aux couvertures des polices
- détection de dépassements de limites de prestations ;
- repérage d'indicateurs potentiels de fraude ou d'erreurs de saisie ;
- identification de données manquantes ou incohérentes.

Ces applications guident les auditeurs à travers le processus d'audit, standardisent les résultats et assurent une piste d'audit complète et traçable.

BÉNÉFICES OBSERVÉS

- Exécution automatisée des tests permettant de passer de plusieurs jours/semaines d'analyse à moins d'une heure pour 37 tests
- Analyse de 100 % des transactions vs échantillonnage lieu d'échantillons, pour une couverture exhaustive
- Détection améliorée des anomalies, incohérences et signaux de fraude grâce à des tests automatisés
- Standardisation du processus d'audit : méthodes homogènes, piste d'audit complète, reproductibilité des analyses
- Recentrage de l'auditeur sur l'analyse et les recommandations, augmentant la valeur ajoutée de l'audit interne

ENSEIGNEMENT CLÉ

- Le cas Allianz Partners illustre une transformation majeure de l'audit interne par la data analytics, avec un passage structurel de l'échantillonnage à l'exhaustivité. CaseWare IDEA démontre qu'il est désormais possible d'analyser 100% des transactions plutôt qu'un échantillon limité, éliminant les angles morts et renforçant considérablement la couverture des risques. Cette approche repositionne fondamentalement le rôle de l'auditeur : moins de temps passé sur les vérifications manuelles répétitives, plus de capacité d'investigation sur les anomalies détectées et de formulation de recommandations stratégiques.

LES FACTEURS CLÉS DE SUCCÈS IDENTIFIÉS

- Standardisation et traçabilité : les applications métier structurent les processus, harmonisent les pratiques et garantissent une documentation complète conforme aux exigences réglementaires.
- Hybridation des compétences : collaboration étroite entre auditeurs (expertise métier) et data analysts (maîtrise technique), nécessitant un investissement significatif en formation
- Gouvernance des données : l'efficacité du système dépend directement de la qualité, complétude et normalisation des données sources en amont.

RECOMMANDATIONS STRATÉGIQUES POUR LA LOD3

TRANSFORMATION DE LA FONCTION AUDIT

La mutation vers l'audit continu doit s'opérer de manière progressive mais déterminée. L'objectif de couvrir 80% du périmètre en audit continu d'ici 2027 nécessite une planification rigoureuse et des investissements significatifs. La création d'une équipe dédiée «Audit Analytics & AI» apporte l'expertise technique nécessaire, tandis que le développement de capacités de simulation et prédiction transforme fondamentalement la valeur ajoutée de la fonction. Un ratio 70/30 entre automatisation et supervision humaine garantit l'efficacité tout en préservant le jugement professionnel indispensable.

NOUVELLES MÉTHODOLOGIES D'AUDIT

L'arsenal méthodologique de l'audit interne s'enrichit de techniques révolutionnaires. Le process mining cartographie les processus réels versus théoriques, révélant les écarts souvent invisibles dans les approches traditionnelles. L'analyse comportementale détecte les anomalies comportementales subtiles qui échappent aux contrôles classiques. L'audit prédictif anticipe les zones de risque avant que les problèmes ne se manifestent. Les tests de stress IA trimestriels évaluent la résilience des systèmes face à diverses contraintes.

REPOSITIONNEMENT STRATÉGIQUE

L'audit interne évolue vers un rôle de conseil stratégique basé sur les analyses IA, devenant un partenaire privilégié de la direction générale. Le partenariat renforcé avec les métiers pour l'amélioration continue transforme la perception traditionnellement défensive de l'audit en approche collaborative. Le leadership sur la gouvernance de l'IA au sein de l'organisation positionne l'audit comme garant de l'utilisation éthique et efficace de ces technologies. La contribution directe à la performance business, avec un objectif d'amélioration de 15% de l'efficacité, légitime les investissements consentis.

L'audit augmenté transforme la posture de la 3e ligne : d'un observateur a posteriori, elle devient un acteur de prévention. L'IA permet d'accélérer les cycles d'audit, d'apporter une assurance plus ciblée et plus pertinente. L'audit du futur repose sur la combinaison de technologies avancées et d'une expertise humaine renforcée.

SYNTHÈSE DES CAS D'USAGES

BNP Paribas, KPMG et Allianz Partners dessinent trois trajectoires complémentaires d'intégration de l'IA dans l'audit interne, révélant un modèle de transformation structurelle convergent. BNP Paribas déploie un assistant virtuel en IA générative pour accélérer l'analyse documentaire, avec une contrainte non négociable : l'hébergement souverain des données sensibles sur infrastructure interne. KPMG intègre l'IA générative dans sa plateforme Clara pour automatiser les tâches à faible valeur ajoutée et enrichir l'analyse financière, positionnant l'IA comme amplificateur d'expertise plutôt que substitut. Allianz Partners mise sur l'audit analytics via CaseWare IDEA pour passer de l'échantillonnage à l'exhaustivité, analysant 100% des transactions et transformant radicalement la couverture des risques.

Trois leviers d'efficacité identiques émergent : gains de productivité massifs (réduction de plusieurs jours à moins d'une heure pour certains processus), amélioration de la détection d'anomalies par analyse systématique, et repositionnement des auditeurs sur l'investigation et la recommandation stratégique. Mais les trois cas convergent surtout sur les conditions critiques de réussite : qualité des données sources (donnée erronée = analyse biaisée), supervision humaine systématique (l'IA assiste, ne décide pas), déploiement progressif avec accompagnement au changement, et gouvernance stricte pour maîtriser les risques éthiques et opérationnels.

Les limites structurelles demeurent : dépendance critique aux données, risques d'hallucinations pour l'IA générative, approche déterministe sans capacité prédictive pour l'analytics, et investissements significatifs en formation et infrastructure. Le modèle qui se dessine n'est ni disruption immédiate ni menace pour les auditeurs, mais transformation maîtrisée où l'IA devient un levier de montée en gamme de la fonction audit, à condition d'être encadrée par une gouvernance responsable et conforme aux exigences réglementaires.

05.

BENCHMARK DES SOLUTIONS IA PAR LOD

Finance Innovation

NEXIALOG CONSULTING

05.1. LOD1

AUGMENTÉE : VERS UN CONTROLE OPERATIONNEL INTELLIGENT

DÉTECTION FRAUDE PAIEMENTS

NETHONE (MANGOPAY GROUP)
(CHALLENGER - BEHAVIORAL BIOMETRICS)
POSITIONNEMENT MARCHÉ : CHALLENGER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Nethone est une solution de prévention de fraude basée sur la biométrie comportementale et l'IA, utilisée par les fintechs, banques et acteurs du paiement en ligne. Elle analyse en temps réel le comportement des utilisateurs (navigation, appareil, interactions) pour détecter les fraudes lors des paiements et des connexions, sans friction pour le client.

LES FONCTIONNALITÉS CLÉS :

- **Biométrie comportementale :** analyse des habitudes de navigation et d'interaction pour identifier les comportements frauduleux
- **Détection de fraude en temps réel :** identification des bots, fraude au paiement, account takeover et multi-comptes
- **Profilage des appareils & utilisateurs :** reconnaissance des devices et création d'empreintes digitales (device fingerprinting)
- **Scoring de risque par IA :** évaluation instantanée du niveau de risque d'une transaction ou d'un utilisateur
- **Prévention des bots et attaques automatisées :** détection du trafic non humain et des scripts malveillants
- **Intégration API :** connexion rapide aux plateformes de paiement, e-commerce et fintech

TECHNOLOGIE CLÉ UTILISÉE

- Behavioral biometrics
- Device fingerprinting
- Unsupervised machine learning
- Deep learning
- Real-time scoring IA
- Network intelligence (Mangopay)
- API / SDK léger

DÉPLOIEMENT ····· ● **Complexité : FAIBLE**

FEEDZAI
(LEADER EU — FRAUDE TEMPS RÉEL)
POSITIONNEMENT MARCHÉ : LEADER EU

DESCRIPTION & FONCTIONNALITÉS CLÉS

Plateforme ML temps réel de détection de fraude financière, spécialisée dans les paiements et le monitoring AML convergé

- **RiskOps Platform :** orchestration centralisée de tous les signaux de fraude (carte, virement, APP, AML)
- **Pulse :** scoring temps réel des transactions avec latence < 100ms
- **Case Manager :** gestion des alertes fraude et AML dans une interface unifiée
- **Genome :** outil d'explication visuelle des décisions IA (XAI) pour équipes fraude
- **Network Analytics :** détection des rings de fraude organisée via graph analytics
- **Behavioral Biometrics :** analyse du comportement de navigation/frappe pour détecter les prises de contrôle de compte (ATO)
- **APP Fraud module :** spécifique à la détection des virements autorisés frauduleux

TECHNOLOGIE CLÉ UTILISÉE

- Machine Learning supervisé
- Graph Neural Networks
- Behavioral biometrics
- Streaming temps réel
- Explainable AI
- Online learning
- Feature store partagé AML +

DÉPLOIEMENT ····· ● **Complexité : ÉLEVÉE**

Le benchmark présenté ci-dessous a été réalisé au Q1 2026 et propose une sélection de solutions IA du marché, en distinguant leaders et challengers, sur les cas d'usage clés de la première ligne (fraude, AML, KYC/onboarding, surveillance opérationnelle). Cette sélection vise à offrir une lecture structurée des options les plus pertinentes à date ; elle reste toutefois évolutive, dans un marché en forte accélération, où de nouvelles solutions peuvent émerger rapidement.

VIREMENT, CARTE, APP FRAUD, FRAUDE EN LIGNE

CAS D'USAGE

CAS 1 — DÉTECTION FRAUDE IDENTITÉ & ATO (ACCOUNT TAKEOVER)

- **Technologies utilisées :** Device Fingerprinting & Behavioral Biometrics
- **Entité :** Leader Buy Now Pay Later (BNPL)
- **Contexte :** L'entité subissait des fraudes à l'identité et des prises de contrôle de compte (ATO) sur son application BNPL. Les fraudeurs utilisaient des identités volées avec des devices propres (jamais vus), contournant les règles basées sur l'historique
- **Action :** Intégration du SDK Nethone sur l'application. Device fingerprinting sur chaque demande de crédit + behavioral biometrics pour détecter les comportements automatisés (bots remplissant des formulaires à vitesse non humaine) et les ATO (comportement de navigation différent du titulaire habituel)
- **Résultat :** −45% fraude à l'identité, −70% ATO, sans friction supplémentaire pour les clients légitimes

CAS 2 — BLOCAGE CARD TESTING

- **Technologies utilisées :** Device Fingerprinting & Behavioral Biometrics temps réel
- **Contexte :** Banque (crédit conso) subissait des fraudes par card testing — des fraudeurs testaient des lots de cartes volées sur le site de paiement pour identifier les cartes actives, avant de les utiliser massivement
- **Action :** Déploiement Nethone pour détecter les comportements de card testing (vitesse de saisie anormale, IP rotative, device fingerprints similaires sur des sessions différentes)
- **Résultat :** −90% card testing détecté et bloqué, économie €1,2M sur 6 mois

POINTS FORTS & AVANTAGES

- Détection de fraude en temps réel grâce à l'IA et à l'analyse du comportement utilisateur
- **Analyse invisible :** aucun impact sur le parcours client, pas d'étapes supplémentaires pour l'utilisateur
- Empreinte appareil très précise (plus de 3000 paramètres analysés) pour identifier utilisateurs et fraudeurs
- Détection efficace des prises de contrôle de comptes (ATO) sans bloquer les clients légitimes
- Détection des bots très élevée (précision annoncée > 99 %)
- **Bénéficie du réseau Mangopay :** partage de signaux de fraude entre plus de 2 500 marchands
- Intégration simple et rapide via un script léger et des API

DÉLAIS — SDK JS côté client : 1-2 semaines — Intégration API score : 2-4 semaines

CAS D'USAGE

CAS 1 — DÉTECTION APP FRAUD SUR VIREMENTS SEPA

- **Technologies utilisées :** ML Comportemental & Scoring temps réel
- **Filiale :** Payment Services
- **Contexte :** Explosion des APP fraud sur les virements SEPA (clients manipulés par téléphone ou phishing pour initier des virements vers comptes fraudeurs). Les règles statiques ne détectaient pas ces virements car le client les initiait lui-même depuis son application
- **Action :** Déploiement du module APP Fraud Feedzai. Modélisation du comportement habituel de chaque client (montants, destinataires, devices, heures). Toute déviation forte génère un score de risque qui peut déclencher une friction (confirmation SMS, appel callback) avant exécution
- **Résultat :** −55% APP fraud sur les virements > 1000€, friction ajoutée sur < 1% des virements légitimes

CAS 2 — DÉTECTION DE FRAUD RINGS CROSS-CANAUX VIA GRAPH ANALYTICS & CONVERGENCE CARTE/VIREMENT

- **Technologies utilisées :** ML Comportemental & Scoring temps réel
- **Contexte :** L'entité traitait la fraude à la carte et la fraude virement sur deux outils distincts, empêchant la détection de fraud rings qui utilisaient à la fois des cartes et des virements
- **Action :** Migration vers Feedzai RiskOps pour convergence des deux flux sur un même modèle de données. Les ring de fraude utilisant carte + virement sont détectés par le module Graph Analytics
- **Résultat :** 3 rings de fraude organisée détectés sur le premier trimestre (impossibles à voir dans les systèmes séparés), économie estimée €2M

POINTS FORTS & AVANTAGES

- Latence scoring < 100ms sur transactions temps réel
- Taux de détection APP fraud > 98%
- Réduction faux positifs de 40-60% vs règles
- **Self-learning :** modèles s'adaptent aux nouvelles typologies
- **Genome :** explicabilité visuelle pour investigateurs
- Traite > $1T de transactions protégées par an

DÉLAIS — Cloud (SaaS) : 3-4 mois — On-premise full : 6-9 mois

05.1. LOD1

AUGMENTÉE : VERS UN CONTROLE OPERATIONNEL INTELLIGENT

TRANSACTION MONITORING AML

QUANTEXA

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Quantexa est une plateforme d'intelligence décisionnelle alimentée par l'IA qui connecte et unifie des données internes et externes fragmentées pour construire une vue contextuelle à 360° des entités (clients, partenaires, transactions).

Grâce à sa technologie de résolution d'entités et d'analyse de graphes, elle détecte automatiquement des relations et comportements cachés entre les données, permettant aux organisations de :

- Détecter les risques, fraudes et menaces en temps réel
- Améliorer la qualité et la fiabilité des données
- Automatiser et augmenter la prise de décision opérationnelle

Elle s'adresse principalement aux secteurs banque, assurance et secteur public, avec des cas d'usage clés en lutte anti-blanchiment (AML), KYC, détection de fraude et gestion du risque client.

TECHNOLOGIE CLÉ UTILISÉE

- Graph Neural Networks
- Machine Learning supervisé + non supervisé
- Natural Language Processing
- Entity Resolution via probabilistic matching
- Streaming temps réel
- Explainable AI

DÉPLOIEMENT ····· **Complexité : ÉLEVÉE**

NICE ACTIMIZE

POSITIONNEMENT MARCHÉ : LEADER MONDIAL

DESCRIPTION & FONCTIONNALITÉS CLÉS

NICE Actimize est une solution RegTech / plateforme SaaS de lutte contre la criminalité financière qui aide les institutions financières à détecter la fraude, surveiller le blanchiment (AML), gérer la conformité (KYC/sanctions), surveiller les marchés financiers et piloter les investigations/cas grâce à des capacités d'IA, d'analytique et de traitement de données en temps réel.

Plateforme AML end-to-end, leader historique avec la suite la plus complète du marché.

TECHNOLOGIE CLÉ UTILISÉE

- Machine Learning (ML)
- Behavioral Analytics
- Anomaly Detection
- Suspicious Activity Monitoring (SAM)
- FRAML (Fraud + AML convergence)
- Entity Risk Scoring / Entity-Centric Analytics
- Real-Time Transaction Monitoring
- Sanctions & PEP Screening
- Fuzzy Matching
- KYC / CDD / EDD Automation
- Case Management (ActOne)
- Workflow Orchestration
- Explainable AI (XAI)
- Rules Engine + AI Hybrid Detection
- Regulatory Reporting Automation (SAR / TRACFIN)

DÉPLOIEMENT ····· **Complexité : ÉLEVÉE**

SURVEILLANCE AUTOMATISÉE DES FLUX EN TEMPS RÉEL

CAS D'USAGE

CAS 1 — LUTTE CONTRE LA FRAUDE OFFSHORE

- **Technologie utilisées :** Graph ML & Entity Resolution
- **Filiale :** CIB (Corporate & Investment Banking)
- **Contexte :** Les équipes compliance détectaient des réseaux de fraude complexes impliquant des fonds illicites transitant via des filiales offshore, mais les systèmes règle-seul généraient 85% de faux positifs
- **Action :** Déploiement du moteur graphe Quantexa pour reconstituer les chaînes de propriété entre entités, comptes et contreparties externes. Le système a identifié des réseaux suspects liés via des dirigeants communs non visibles dans les données transactionnelles seules.
- **Résultat :** −45% faux positifs, +30% détection cas à soumettre TRACFIN

CAS 2 — DÉTECTION D'ANOMALIES COMPORTEMENTALES MULTI-PAYS

- **Technologie utilisées :** Graph ML
- **Contexte :** Monitoring correspondent banking sur plusieurs pays avec des règles statiques inadaptées aux variations de comportement par région
- **Action :** Graph analytics pour détecter anomalies comportementales cross-frontières, avec enrichissement automatique registres d'entreprises locaux
- **Résultat :** Réduction de 60% du temps d'investigation par analyste

POINTS FORTS & AVANTAGES

- Détection de risques cachés via graphe de connaissances et analyse réseau
- **Entity Resolution :** +90% de précision, beaucoup plus rapide que les approches traditionnelles
- Vue 360° client enrichie en temps réel (sanctions, PEP, registres, actualités)
- IA explicable et auditable — conforme aux exigences réglementaires (ACPR, EBA)
- Réduction drastique des faux positifs grâce à l'analyse contextuelle

DÉLAIS On-premise : 6-12 mois · Cloud : 3-6 mois

CAS D'USAGE

CAS 1 — FRAUDE & AML CONVERGENCE FRAML & GESTION DE CAS UNIFIÉE

- **Technologies utilisées :** via Rule-Based ML & ERCM
- **Filiale :** filiale exposée aux flux transfrontaliers
- **Contexte :** Les équipes Fraud et AML travaillaient sur des systèmes séparés, générant des doublons d'alertes et des incohérences dans les rapports SAR.
- **Action :** Déploiement du module FRAML convergé (Xceed) + ERCM (Enterprise Risk Case Management). Unification des alertes des deux équipes dans une seule interface.
- **Résultat :** Doublons éliminés, rapports SAR cohérents, réduction du temps de traitement par dossier de 35%.

CAS 2 — RÉDUCTION DES FAUX POSITIFS AML SUR OPÉRATIONS DE MARCHÉ

- **Technologies utilisées :** ML comportemental (SAM)
- **Contexte :** Volume croissant d'alertes AML sur les opérations de marché, avec un taux de faux positifs > 90% sur le système legacy.
- **Action :** Migration vers SAM avec ML comportemental calibré sur les typologies marché (wash trading, structuring obligations). Déploiement ActOne pour gestion de cas.
- **Résultat :** −55% faux positifs, temps d'enquête par analyste réduit de 40%

POINTS FORTS & AVANTAGES

- **SAM** → +40% suspicious tx détectées vs règles seules
- **KYC** → −60% charge manuelle EDD grâce à l'automatisation
- **Sanctions** → −50% faux positifs par correspondance IA
- **FRAML** → −80% overlap faux positifs Fraud/AML
- **XAI** → auditabilité totale ACPR / régulateurs
- **Cloud SaaS AWS** → déploiement < 3 mois
- **Réseau sécurisé** → $6T de transactions protégées/jour

DÉLAIS On-premise : 12-18 mois · SaaS AWS (Xceed) : 3-6 mois

05.1. LOD1

AUGMENTÉE : VERS UN CONTROLE OPERATIONNEL INTELLIGENT

KYC & ONBOARDING CLIENT AUTOMATISÉ

ONFIDO (ENTRUST)

POSITIONNEMENT MARCHÉ : LEADER EU
ACQUIS PAR ENTRUST (2024)

DESCRIPTION & FONCTIONNALITÉS CLÉS

Onfido (désormais intégré à Entrust Identity Verification) est une solution d'IA de vérification d'identité à distance qui permet de confirmer qu'une personne est bien réelle en analysant sa pièce d'identité et ses biométries faciales (selfie/visage), afin de sécuriser l'onboarding, réduire la fraude et répondre aux exigences de conformité (KYC/AML).

TECHNOLOGIE CLÉ UTILISÉE

- Machine Learning (ML)
- Deep Learning
- Computer Vision
- Face Recognition / Face Matching
- Biometric Verification
- Liveness Detection (anti-spoofing)
- Motion Liveness / Motion Analysis
- OCR (Optical Character Recognition)
- Anomaly Detection
- Risk Scoring / Decision Engine
- Fuzzy Matching
- Image Forensics
- Fraud Signal Detection
- AI-assisted Capture SDK / Smart Capture
- NFC reading (sur documents compatibles)

DÉPLOIEMENT ····· **Complexité : FAIBLE**

IDNOW

POSITIONNEMENT MARCHÉ : LEADER EU

DESCRIPTION & FONCTIONNALITÉS CLÉS

IDnow Plateforme KYC européenne complète couvrant tous les niveaux d'assurance eIDAS, du selfie automatique à la vidéo-ident avec opérateur humain.

- **AutoIdent :** vérification identité automatique (IDV + biométrie) pour niveau Faible/Substantiel
- **VideoIdent :** vérification avec opérateur humain pour niveau Élevé eIDAS (banque, assurance-vie)
- **eSign (signature électronique) :** qualifiée eIDAS, intégrée au parcours KYC
- **AML Suite :** screening PEP/sanctions intégré post-IDV
- **Identity Wallet :** stockage sécurisé des documents vérifiés pour réutilisation
- **B2B Verification :** vérification dirigeants d'entreprise + UBO

TECHNOLOGIE CLÉ UTILISÉE

- Computer Vision
- Biométrie faciale avec liveness detection
- NLP
- Cryptographie eIDAS
- Modèles de détection de fraude documentaire
- Infrastructure certifiée ISO 27001, SOC

DÉPLOIEMENT ····· **Complexité : MODÉRÉE**

VÉRIFICATION IDENTITÉ ET CONFORMITÉ LCB-FT

CAS D'USAGE

CAS 1 — AUTOMATISATION KYC

- **Technologies utilisées :** Computer Vision,Machine Learning (ML),Deep Learning,Face Matching / Biométrie faciale, Liveness Detection (anti-spoofing)Risk Scoring / Decision Engine
- **Entité :** Banque en ligne
- **Contexte :** Automatiser à 100% le parcours KYC d'ouverture de compte, qui nécessitait encore une validation manuelle des documents pour 30% des dossiers
- **Action :** Déploiement du SDK Onfido intégré dans l'app mobile. Vérification document (carte d'identité + passeport) + liveness check + NFC pour passeports biométriques. Les dossiers validés automatiquement par Onfido passent directement à l'activation
- **Résultat :** 95% des ouvertures de compte validées sans intervention humaine, temps moyen de vérification réduit à 2min30, fraude identitaire détectée +40% vs ancien système

CAS 2 — KYC UNIFIÉ MULTI-PAYS

- **Technologies utiliées :** ML documentaire & Rule Engine configurable
- **Contexte :** L'entité cherchait à unifier son parcours KYC sur 4 pays avec une solution unique conforme aux réglementations locales de chaque pays
- **Action :** Déploiement Onfido avec configuration pays par pays des règles de validation documentaire. Intégration dans le back-office via API
- **Résultat :** Un seul outil KYC pour 4 pays, conformité AMLD5 validée dans chaque juridiction, onboarding unifié en < 5 minutes

POINTS FORTS & AVANTAGES

- Taux d'acceptation automatique > 92% (référence industrie)
- Couverture 2500+ documents dans 195 pays
- Détection deepfake et injection vidéo (leader marché)
- **UX mobile optimisée :** < 3 minutes pour vérification complète
- Taux conversion onboarding parmi les plus élevés du marché

DÉLAIS — SDK mobile : 2-4 semaines — Intégration API full : 1-2 mois

CAS D'USAGE

CAS 1 — ONBOARDING 100% DIGITAL EN TOUTE CONFORMITÉ

- **Technologies Utilisées :** OCR, Liveness Detection & Screening AML (AutoIdent/VideoIdent)
- **Entité :** Pôle digital pour l'onboarding
- **Contexte :** Le pôle devait proposer un onboarding 100% digital conforme LCB-FT avec niveau d'assurance Substantiel (requis par l'ACPR pour ouverture de compte à distance), tout en maintenant un taux de conversion > 80%
- **Action :** Intégration IDnow AutoIdent dans le tunnel d'onboarding digital. Parcours : vérification CNI/passeport + liveness check + screening AML intégré. Pour les cas complexes (UBO d'entreprise), bascule automatique vers VideoIdent
- **Résultat :** 87% de conversion sur le parcours automatique, délai moyen 4 minutes, conformité ACPR validée en audit

CAS 2 — DÉMATÉRIALISATION ASSURANCE-VIE

- **Technologies Utilisées :** VideoIdent & eSign qualifiée
- **Contexte :** La souscription d'un contrat d'assurance-vie nécessitait légalement un niveau d'assurance ÉlevéeIDAS pour les montants > 150k€, impossible à atteindre avec un simple selfie automatique
- **Action :** Déploiement IDnow VideoIdent pour les parcours assurance-vie > 150k€ et pour les rachats importants. Intégration dans le SI avec signature électronique qualifiée IDnow eSign
- **Résultat :** 100% des souscriptions dématérialisées sans dépôt physique, conformité Solvabilité II + LCB-FT maintenue

POINTS FORTS & AVANTAGES

- Seul acteur couvrant TOUS les niveaux eIDAS (Faible → Qualifié)
- **VideoIdent :** niveau Élevé requis pour certains produits bancaires et assuranciels
- eSign qualifiée intégrée = parcours sans rupture
- Conforme AMLD5, DSP2, Solvabilité II
- 24/7 opérateurs multilingues pour VideoIdent

DÉLAIS — AutoIdent (automatique) : 4-6 semaines — VideoIdent + eSign : 2-4 mois

05.2. LOD2

A L'ÈRE DE L'IA : RISQUES & CONFORMITÉ EN PLEINE MUTATION

REPORTING RÉGLEMENTAIRE

REGNOLOGY

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Solution RegTech de Regnology pour automatiser le reporting réglementaire, la conformité et la gestion des données des institutions financières et régulateurs.

FONCTIONNALITÉS CLÉS

- Automatisation du reporting réglementaire multi-juridictions (XBRL, XML, etc.)
- Collecte, validation et transformation des données pour améliorer leur qualité
- Plateforme cloud unifiée avec workflows de conformité et tableaux de bord
- **Modules spécialisés :** reporting financier, transactionnel, fiscal et risques

TECHNOLOGIE CLÉ UTILISÉE

- **Cloud (hébergement en ligne) :** la solution fonctionne sur des serveurs cloud (notamment Google Cloud), ce qui permet d'y accéder à distance, de stocker beaucoup de données et de s'adapter facilement au volume de reporting
- **Standards de données réglementaires (XBRL, XML) :** Regnology utilise des formats standard pour structurer les données financières et réglementaires afin qu'elles soient lisibles automatiquement par les régulateurs
- **Architecture modulaire (microservices & API) :** la plateforme est composée de petits modules indépendants qui peuvent être mis à jour ou connectés facilement aux systèmes internes des banques
- **Automatisation et contrôles de données :** la technologie permet de collecter, vérifier et transformer automatiquement les données pour éviter les erreurs manuelles
- **IA et outils d'analyse :** certaines fonctions utilisent l'IA pour aider à analyser les données, automatiser des tâches et améliorer le suivi réglementaire

DÉPLOIEMENT ····· **Complexité : MODÉRÉE**

AXIOM SL

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

AxiomSL est une plateforme logicielle leader mondial dédiée au reporting réglementaire et à la gestion des risques.

Elle sert de pont entre les données brutes d'une institution financière et les exigences complexes des régulateurs mondiaux (Bâle III/IV, liquidité, reporting transactionnel, etc.)

Son cœur est la plateforme ControllerView®, qui centralise le contrôle des données pour garantir qu'elles sont correctes, traçables et conformes avant d'être envoyées aux autorités.

TECHNOLOGIE CLÉ UTILISÉE

- **Machine Learning (ML) & Data Quality :** Des algorithmes de ML analysent les flux de données entrants pour identifier des «outliers» (valeurs aberrantes) ou des modèles inhabituels avant qu'ils n'impactent les rapports
- **Natural Language Processing (NLP) & Veille Réglementaire :** Utilisation du NLP pour scanner et interpréter automatiquement les textes de lois et publications des régulateurs mondiaux
- **Robotic Process Automation (RPA) & Orchestration :** Automatisation des tâches répétitives comme la collecte de fichiers, le lancement des calculs et la distribution des rapports

DÉPLOIEMENT ····· **Complexité : ÉLEVÉE**

Axé sur les fonctions Risques et Conformité, ce benchmark analyse les solutions IA les plus pertinentes sur plusieurs cas d'usage structurants : reporting réglementaire multi-juridictions, modélisation du risque de crédit (IFRS 9, stress testing) et gestion du risque opérationnel (GRC).

Les solutions sélectionnées ont été appréciées selon leur capacité à répondre aux exigences prudentielles en vigueur, notamment Bâle IV, DORA et CSRD, et à s'intégrer dans des architectures et organisations complexes. Ce panorama demeure évolutif, sous l'effet combiné de l'intensification des contraintes réglementaires et de la diffusion croissante de l'IA dans les dispositifs de conformité.

CAS D'USAGE

CAS 1 — PLATEFORME UNIQUE POUR LES REPORTING RÉGLEMENTAIRE MULTI-RÉGULATEURS

- **Technologie utilisées :** Rule-based engine, automatisation XBRL, collecte données centralisée
- **Contexte :** Transformation du reporting réglementaire et choix d'une plateforme unique pour tous les reportings. Déploiement Abacus360 Banking de Regnology après un processus de sélection complet
- **Solutions utilisées :** Plateforme Abacus360 Banking comme outil central de reporting ; Modules Abacus complémentaires pour collecte de données, génération de cash-flows et tests réglementaires
- **Bénéfices observés :** Réduction des délais de production des reportings ; Automatisation et industrialisation des processus ; Amélioration de la qualité et de la réactivité du reporting ; Meilleure anticipation des évolutions réglementaires

CAS 2 — AUTOMATISATION DES PROCESSUS MANUELS DES REPORTING REGLEMENTAIRES

- **Technologies utilisées :** Rule-based engine, connecteurs SAP/Murex, validation XBRL automatisée
- **Contexte :** Besoin de consolider les reportings réglementaires de plus de 40 entités dans 15 pays pour plusieurs régulateurs (ACPR, BCE…) ; Processus manuel lourd mobilisant 25 ETP pendant 3 semaines chaque trimestre
- **Solutions utilisées :** Regnology Reporting Factory ; Connecteurs directs aux systèmes internes (SAP, Murex) ; Automatisation COREP/FINREP et validation XBRL avant soumission
- **Bénéfices observés :** Production réduite de 3 semaines à 4 jours ; Effectifs mobilisés réduits de 25 à 8 ETP ; Aucun rejet ACPR lié au format depuis le déploiement

POINTS FORTS & AVANTAGES

Leader international des solutions de reporting réglementaire et de supervision financière;
Présent dans plus de 100 pays et utilisé par banques, assureurs et autorités de régulation.

Les avantages et points forts :

- Automatisation du reporting réglementaire, réduisant les tâches manuelles et les erreurs
- Plateforme unifiée couvrant plusieurs réglementations et juridictions
- Amélioration de la qualité, traçabilité et cohérence des données
- Gain de temps et réduction des coûts de conformité
- Adaptation rapide aux évolutions réglementaires
- Solutions modulaires intégrables aux systèmes existants

DÉLAIS ····· Cloud SaaS : 3-4 mois ····· On-premise : 6-12 mois

CAS D'USAGE

CAS 1 — REDUCTION DU TEMPS DE CALCUL DES RATIOS DE LIQUIDITÉ

- **Technologies utilisées :** Moteur de calcul in-memory, connecteurs Murex/Kondor, What-If analysis temps réel
- **Contexte :** Consolidation reporting multi-entité avec un focus sur les ratios LCR/NSFR
- **Solution utilisées :** Produit : AxiomSL ControllerView® avec moteur de calcul in-memory haute performance ; Modules : Calcul et Reporting réglementaire de liquidité (LCR / NSFR)
- **Intégration :** Mise en place de connecteurs directs pour une alimentation automatique depuis les systèmes ALM existants (Murex, Kondor)
- **Bénéfices Observés :** Performance : Réduction drastique du temps de calcul du LCR groupe, passant de 18 heures à 45 minutes ; Agilité : Capacité nouvelle de simuler des scénarios de stress tests en temps réel (What-If analysis) ; Conformité : Fiabilité accrue des données soumises, avec zéro rejet de la part de la BCE sur une période de 3 ans

CAS 2 — RÉFÉRENTIEL UNIQUE MULTI-RÉGULATEURS

- **Technologies utilisées :** Rule-based mapping, référentiel données centralisé, automatisation XBRL multi-juridictions
- **Contexte :** Périmètre : Harmonisation des reportings réglementaires entre les entités Banque d'Investissement et Gestion d'Actifs
- **Solution utilisées :** Produit : AxiomSL ControllerView® déployé comme Hub Central de Reporting ; Fonctionnalité Clé : Mise en place d'un référentiel de données unique avec mapping automatique entre les formats locaux des entités et les standards des régulateurs (EBA, SEC)
- **Bénéfices utilisées :** Efficacité Opérationnelle : Création d'un référentiel unique capable de servir simultanément 3 régulateurs majeurs -- ACPR (France), FCA (UK), et SEC (USA) ; Qualité des Données : Réduction de 60% des réconciliations manuelles, diminuant significativement le risque d'erreur opérationnelle ; Consistance : Garantie d'une cohérence des données reportées entre les différentes juridictions

POINTS FORTS & AVANTAGES

- **Connectivité Native :** Connexion directe aux sources hétérogènes, sans modèle imposé
- **Data Lineage :** Traçabilité granulaire du rapport jusqu'à la source brute
- **Veille Réglementaire :** Mises à jour automatiques des règles, conformité continue sans effort interne
- **Plateforme Unifiée :** Multi-juridictionnel et multi-domaine sur une seule instance
- **Flexibilité Métier :** Règles paramétrables par les métiers, peu de dépendance IT
- **Scalabilité :** Conçu pour les très gros volumes et les institutions Tier 1

DÉLAIS ····· Core déploiement : 6-9 mois ····· Full scope multi-régulateur : 12-18 mois

05.2. LOD2

A L'ÈRE DE L'IA : RISQUES & CONFORMITÉ EN PLEINE MUTATION

RISQUE CRÉDIT

MOODY'S ANALYTICS

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Plateforme analytique de Moody's dédiée à la gestion du risque de crédit, au calcul des pertes attendues (ECL/IFRS 9) et au stress-testing réglementaire.

Permet aux banques et institutions financières de mesurer, prévoir et piloter les risques financiers en intégrant données, modèles et scénarios économiques.

LES FONCTIONNALITÉS CLÉS

- **Calcul IFRS 9 / ECL automatisé :** modèles enrichis par l'IA pour mieux estimer les pertes de crédit attendues et les provisions
- **Modélisation avancée du risque de crédit :** machine learning pour affiner la probabilité de défaut, la perte et l'exposition
- **Scénarios macroéconomiques prédictifs :** IA utilisée pour anticiper l'impact des évolutions économiques sur les portefeuilles
- **Stress-testing intelligent :** simulations plus rapides et plus précises grâce aux modèles analytiques automatisés
- **Qualité et analyse des données :** IA pour détecter anomalies, améliorer la fiabilité et enrichir les données de risque
- **Reporting automatisé et aide à la décision :** génération de rapports et analyses prédictives pour appuyer les décisions de gestion des risques

TECHNOLOGIE CLÉ UTILISÉE

- **Intelligence artificielle & machine learning :** modèles prédictifs pour le risque de crédit, IFRS 9 et stress-testing
- **Big data & bases de données financières :** exploitation de larges volumes de données historiques (défauts, marchés, macroéconomie)
- **Modélisation statistique avancée :** PD, LGD, EAD, simulations économiques et financières
- **Plateformes cloud et SaaS :** accès aux solutions et calculs via des environnements sécurisés en ligne
- **Outils de scénarios économiques :** moteurs de simulation macroéconomique et prévisionnels intégrés
- **API & intégration systèmes :** connexion aux systèmes bancaires internes (finance, risque, comptabilité)

DÉPLOIEMENT ····· **Complexité : MODÉRÉE à ÉLEVÉE**

SAS CREDIT RISK

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Solution analytique intégrée dédiée à la mesure, modélisation et pilotage du risque de crédit pour les banques et institutions financières. **Elle permet de couvrir le cycle complet :** estimation du risque, provisionnement (IFRS 9/CECL), stress-testing et reporting réglementaire.

LES FONCTIONNALITÉS CLÉS

- **Modélisation du risque de crédit :** machine learning pour améliorer la prédiction de défaut (PD), perte (LGD) et exposition (EAD)
- **Scoring et décision crédit :** algorithmes d'IA pour évaluer le profil de risque des clients et affiner l'octroi
- **IFRS 9 / ECL prédictif :** modèles IA pour estimer les pertes futures selon différents scénarios économiques
- **Détection de risques et anomalies :** identification de signaux faibles de dégradation du crédit dans les portefeuilles
- **Stress-testing avancé :** simulations économiques plus précises grâce aux modèles analytiques automatisés
- **Automatisation analytique :** génération automatique d'analyses et de reportings basés sur les données et modèles

TECHNOLOGIE CLÉ UTILISÉE

- **Machine learning & économétrie :** modèles prédictifs et IFRS 9 forward-looking (PD, LGD, ECL, modèles satellite macroéconomiques)
- **Simulations Monte Carlo :** projection du risque de portefeuille et stress-testing réglementaire
- **Explainable AI (IA explicable) :** modèles transparents et auditables pour validation réglementaire (IRB, IFRS 9)
- **In-memory analytics (SAS Viya / LASR) :** calculs rapides sur de très grands volumes de données et portefeuilles
- **Deep learning & NLP (selon cas) :** utilisés pour analyses avancées et exploitation de données non structurées
- **Intégration data & API :** connexion aux systèmes bancaires (finance, risque, CRM) et aux bases de données internes

DÉPLOIEMENT ····· **Complexité : ÉLEVÉE**

IFRS 9 / ECL MODELLING / STRESS-TESTING / CREDIT PORTFOLIO MANAGEMENT

CAS D'USAGE

CAS 1 — AUTOMATISATION CALCUL ECL IFRS 9

- **Technologies utilisées :** ML supervisé (modèles PD/LGD), intégration scénarios macro, automatisation calcul ECL
- **Contexte :** Application d'IFRS 9 imposant le calcul des pertes attendues (ECL) sur ~800 Md€ d'encours ; Intégration obligatoire de 3 scénarios macroéconomiques pondérés ; Système legacy inadapté aux calculs macro-conditionnels
- **Solution utilisée :** Déploiement de ImpairmentStudio (Moody's Analytics) ; Intégration des prévisions macroéconomiques internes ; Modèles PD/LGD calibrés sur données historiques internes + benchmarks Moody's ; Automatisation complète du calcul ECL sur le portefeuille groupe
- **Bénéfices observés :** Conformité IFRS 9 atteinte avant l'échéance réglementaire ; Calcul des provisions en 4 heures (vs 3 semaines auparavant) ; Validation Big Four sans observation majeure.

CAS 2 — OPTIMISATION RECOUVREMENT NPL

- **Technologies utilisées :** ML supervisé (scoring recouvrement), ML non supervisé (segmentation), optimisation stratégie
- **Contexte :** Hausse de +30 % des prêts non performants (NPL) sur le portefeuille PME ; Nécessité d'une segmentation fine pour optimiser recouvrement, restructuration ou cession
- **Solution utilisée :** Utilisation de NPL Analytics (Moody's Analytics) ; Segmentation selon probabilité de recouvrement, profil financier et garanties ; Modèles de machine learning pour identifier la stratégie maximisant le taux de recouvrement
- **Bénéfices observés :** +15 % de taux de recouvrement vs stratégie uniforme ; −20 % de coûts de recouvrement ; Cession d'actifs non récupérables à +8 % vs estimation initiale

POINTS FORTS & AVANTAGES

- Expertise reconnue mondialement en risque de crédit et modélisation financière
- Données propriétaires étendues (défauts, transitions de notation, données macroéconomiques)
- Modèles robustes conformes aux exigences réglementaires (IFRS 9, stress-tests BCE, etc.)
- **Intégration complète :** données + modèles + scénarios + reporting
- Capacité de simulation multi-scénarios pour anticiper les crises économiques
- Solutions cloud sécurisées et facilement intégrables aux systèmes bancaires
- Amélioration de la précision des provisions et de la prise de décision

DÉLAIS ····· Implémentation IFRS 9 : 4-9 mois ····· Modèles sur-mesure : +3-6 mois

CAS D'USAGE

CAS 1 —AUTOMATISATION STRESS-TESTING ICAAP

- **Technologies utilisées :** ML supervisé (modèles macro), simulation Monte Carlo, automatisation calcul capital
- **Contexte :** Réalisation de l'ICAAP annuel sur ~500 Md€ d'actifs avec scénarios de stress personnalisés ; Obligation de remise des résultats à l'ACPR en 6 semaines ; Besoin d'automatiser les simulations d'impact sur les fonds propres
- **Solution utilisée :** Déploiement SAS Stress Testing ; Modèles macroéconomiques calibrés sur données françaises (PIB, chômage, immobilier) ; Automatisation du calcul d'impact sur capital par segment de portefeuille
- **Bénéfices observés :** Délai ICAAP réduit de 12 à 5 semaines ; Analyses de sensibilité quasi en temps réel ; Aucune observation ACPR sur la méthodologie

CAS 2 — DÉTECTION DÉFAUTS PME/ETI

- **Technologies utilisées :** ML supervisé + non supervisé, NLP (presse/INPI), scoring mensuel automatisé , (SAS Early Warning)
- **Contexte :** Volonté de détecter les entreprises à risque 6 à 12 mois avant défaut ; Objectif : anticiper restructurations et limiter pertes de crédit
- **Solution utilisée :** Déploiement SAS Early Warning System ; Modèles machine learning combinant données internes (comptes, crédit) et externes (Banque de France, INPI, presse) ; Scoring mensuel du portefeuille PME/ETI
- **Bénéfices observés :** 78 % des défauts détectés environ 9 mois à l'avance ; −35 % de passages directs en défaut sévère (Stage 3) ; Meilleure anticipation des provisions IFRS 9

POINTS FORTS & AVANTAGES

- Plateforme analytique complète couvrant tout le cycle du risque de crédit (octroi, provisionnement, stress-tests, reporting)
- Forte capacité de modélisation avancée (statistiques, machine learning, économétrie)
- Modèles explicables conformes aux exigences réglementaires (IFRS 9, Bâle, IRB)
- Traitement rapide de très grands volumes de données grâce à l'in-memory analytics
- Automatisation des calculs et des reportings réglementaires
- Intégration facile aux systèmes bancaires existants
- Réduction du risque d'erreur et amélioration de la qualité des décisions de crédit

DÉLAIS ····· Core scoring/IFRS9 : 6-9 mois ····· Full suite MRM + stress test : 12-18 mois

05.2. LOD2

A L'ÈRE DE L'IA : RISQUES & CONFORMITÉ EN PLEINE MUTATION

RISQUE OPÉRATIONNEL

METRICSTREAM

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

MetricStream est une plateforme intégrée de Gestion des Risques et de la Conformité (GRC), utilisée pour piloter les risques opérationnels, informatiques et réglementaires.

Elle centralise la cartographie des risques, automatise la collecte des incidents et utilise l'intelligence artificielle (AiSPIRE) pour détecter les doublons, classifier les événements et optimiser les contrôles, offrant ainsi une vision unifiée et dynamique de l'exposition aux risques de l'entreprise.

TECHNOLOGIE CLÉ UTILISÉE

- **MetricStream Platform (socle technologique) :** Plateforme cloud-native flexible permettant de construire et déployer des applications GRC
- **Architecture Low-Code / No-Code :** Permet aux équipes métier d'adapter les formulaires et les workflows sans développement informatique lourd
- **Intelligence Artificielle & Machine Learning (AiSPIRE) :**
  - NLP (Natural Language Processing) : Pour la classification automatique des incidents (Issues) et la détection de doublons sémantiques dans les contrôles et risques
  - Machine Learning : Pour la recommandation intelligente d'actions correctives basées sur l'historique des données
  - Generative AI (GenAI) : Intégration récente pour l'assistance conversationnelle (chatbot) et la synthèse de documents réglementaires
  - Analytique & Reporting : Tableaux de bord intégrés avec capacités de visualisation de données pour le pilotage des risques en temps réel

DÉPLOIEMENT ····· **Complexité : MODÉRÉE à ÉLEVÉE**

IBM OPENPAGES (LEADER GRC ANALYTIQUE)

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Plateforme GRC (Governance, Risk & Compliance) avec des capacités analytiques avancées pour la gestion du risque opérationnel et la conformité réglementaire.

Elle sert à identifier, surveiller et atténuer tous les risques de l'entreprise au même endroit, le tout boosté par l'Intelligence Artificielle d'IBM (Watson).

TECHNOLOGIE CLÉ UTILISÉE

- **IBM Watson NLP :** classification automatique des incidents par type de risque (Bâle IV)
- Machine Learning pour prédiction des pertes opérationnelles et détection d'anomalies
- Generative AI (IBM WatsonX) pour aide à la rédaction des plans de remédiation et des rapports
- Graph analytics pour analyse d'impact des incidents ICT
- Rules engine pour suivi automatique des obligations réglementaires
- **API REST + connecteurs IBM natifs**

DÉPLOIEMENT ····· **Complexité : MODÉRÉE à ÉLEVÉE**

CAS D'USAGE

CAS — CRÉATION D'UNE BIBLIOTHÈQUE UNIQUE DES CONTROLES IT DE CONTRÔLES UNIFIÉE & RISK ASSESSMENT AUTOMATISÉ

- **Technologies utilisées :** Rule-based (bibliothèque contrôles), automatisation campagnes évaluation, dashboard temps réel
- **Contexte & Problématique :** Périmètre : Gestion des Risques Informatiques (IT Risk) et de la Conformité au niveau Groupe ; Défi Majeur : Avec des milliers d'applications et d'infrastructures à travers le monde, la banque avait besoin d'harmoniser ses évaluations de risques IT. Les processus manuels ou disparates rendaient difficile la vision consolidée de l'exposition au risque cyber et technologique exigée par la BCE
- **Solution utilisée :** Produit : MetricStream IT & Cyber Risk Management ; Fonctionnalité Clé : Déploiement d'une bibliothèque unique de contrôles IT et automatisation des campagnes d'évaluation des actifs (Risk Assessment)
- **Bénéfices Observés :** Visibilité : Vue unifiée et temps réel de la posture de risque IT sur l'ensemble du groupe ; Efficacité : Réduction du temps passé par les correspondants risques à collecter les preuves de contrôles ; Pilotage : Capacité à prioriser les investissements de sécurité sur les zones les plus critiques identifiées par l'outil

POINTS FORTS & AVANTAGES

- **Approche Platform-First (PaaS) :** Architecture modulaire et scalable permettant de déployer progressivement des cas d'usage (ex: commencer par le Risque Opérationnel, puis ajouter le Cyber Risk) sans complexité
- **Intelligence Artificielle «AiSPIRE» :** Moteur d'IA intégré spécialisé dans l'efficacité opérationnelle (détection automatique de doublons, classification intelligente des incidents, suggestions de contrôles)
- **Intégration Frontline (LOD 1) :** Expérience utilisateur pensée pour faciliter l'adoption par les métiers (première ligne de défense), avec des interfaces simplifiées et mobiles
- **Low-Code / No-Code :** Grande flexibilité de configuration permettant aux administrateurs fonctionnels d'adapter les workflows et formulaires sans dépendance forte à l'IT
- **Écosystème Connecté :** Capacité native à s'interfacer avec les outils de sécurité (ex: Qualys), de gestion de services (ServiceNow) et les flux de données externes (ex: Dow Jones pour la veille)
- **Contenu Réglementaire (Unified Compliance Framework) :** Accès intégré à une bibliothèque massive de contenus réglementaires et standards (ISO, NIST, RGPD) mis à jour régulièrement

DÉLAIS ····· Moyenne : 6-12 mois, la périodicité varie selon le périmètre du projet

CAS D'USAGE

CAS 1 — OPTIMISATION DES PROCESSUS DE COLLECTE DES INCIDENTS

- **Technologies utilisées :** IBM OpenPages ORM | Rule-based (SMA), API multi-entités, reporting ACPR
- **Contexte & Problématique :** 18 fédérations aux outils disparates, incapables de consolider fiablement les pertes opérationnelles pour répondre aux exigences SMA de Bâle IV
- **Solution utilisées :** Référentiel unique via IBM OpenPages ORM, connecté aux 18 fédérations par API pour automatiser collecte et calcul SMA
- **Bénéfices Observés :** Déploiement en 6 mois ; Complétude des données : 60% → 95% ; Reporting ACPR entièrement automatisé

CAS 2 — AMÉLIORATION DU TEMPS D'ANALYSES DES CONTRATS FOURNISSEURS ICT

- **Technologies utilisées :** IBM OpenPages TPRM | NLP Watson, ML scoring, Rule-based DORA
- **Contexte & Problématique :** 400 contrats fournisseurs ICT à analyser pour DORA, avec une estimation manuelle de 18 mois, incompatible avec les échéances réglementaires
- **Solution utilisée :** IBM OpenPages TPRM avec Watson NLP pour extraire automatiquement les clauses ICT et scorer la criticité selon les critères DORA
- **Bénéfices Observés :** Analyse complète en 3 mois (vs 18 mois manuellement) ; 12 fournisseurs critiques identifiés pour remédiation immédiate ; Équipes juridiques libérées des tâches fastidieuses

POINTS FORTS & AVANTAGES

- **Vision à 360° des Risques :** Casse les silos entre risque informatique, opérationnel et conformité
- **IA Intégrée (Watson) :** Lecture automatique des documents, détection de l'efficacité des contrôles et suggestion d'actions
- **Automatisation des Workflows :** Gestion automatique des validations, revues d'audit et alertes en cas de dépassement de seuil
- **Tableaux de Bord Dynamiques :** Visualisation en temps réel des vulnérabilités pour la direction générale

DÉLAIS ····· OpenPages ORM : 4-6 mois ····· Module DORA + Third-Party : 6-9 mois

05.3. LOD3

L'AUDIT DU FUTUR : COMMENT L'IA TRANSFORME LA 3E LIGNE DE DEFENSE

AUDIT INTERNE / MONITORING CONTINU

GALVANIZE / DILIGENT HIGHBOND (LEADER CONTINUOUS MONITORING)

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Plateforme de continuous monitoring et d'audit interne basée sur l'automatisation des tests de contrôle en temps réel.

- **Continuous Control Monitoring (CCM) :** exécution automatique et continue des tests de contrôle sur les données de production
- **Automated Testing Engine :** 500+ tests préconfigurés couvrant les processus financiers, achats, paie, IT
- **Anomaly Detection :** ML pour détecter les transactions suspectes et les exceptions dans les données
- **Risk Heatmap en temps réel :** tableau de bord du profil de risque mis à jour automatiquement
- **Issue Management :** workflow de traitement des exceptions avec escalade automatique
- **Audit Trail :** traçabilité complète de tous les tests et résultats pour les régulateurs
- **ACL Analytics intégré :** outil d'analyse de données pour les auditeurs (requêtes sur millions de lignes)

TECHNOLOGIE CLÉ UTILISÉE

- Machine Learning
- Rules engine
- NLP (Diligent AI)
- Generative AI pour rédaction automatique des constats et recommandations d'audit
- Statistical sampling pour sélection intelligente d'échantillons d'audit

DÉPLOIEMENT ····· **Complexité : FAIBLE à MODÉRÉE**

MINDBRIDGE AI AUDITOR (CHALLENGER IA — DÉTECTION ANOMALIES)

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

Premier outil d'audit basé sur l'IA générative et le ML pour l'analyse exhaustive des journaux comptables et la détection d'anomalies financières.

- **AI Risk Engine :** analyse 100% des écritures comptables via ML pour identifier les transactions à risque
- **Continuous Ledger Monitoring :** surveillance continue des journaux GL avec scoring de risque par écriture
- **Outlier Detection :** identification des transactions atypiques par rapport aux patterns normaux
- **Journal Entry Testing (JET) :** test automatique des saisies manuelles suspectes (SOX, IFRS)
- **Fraud Indicators :** 25 indicateurs de fraude financière préconfigurés
- **Natural Language Queries :** les auditeurs interrogent les données en langage naturel
- **Sampling Intelligence :** priorisation des transactions à investiguer par niveau de risque

TECHNOLOGIE CLÉ UTILISÉE

- Machine Learning supervisé
- Isolation Forest et Local Outlier Factor pour détection anomalies multidimensionnelles
- NLP
- Generative AI (GPT-4 intégré) pour analyse contextuelle et génération d'hypothèses d'audit
- Unsupervised clustering pour segmentation des comportements comptables normaux
- **Statistical profiling :** distribution analysis sur les montants, comptes, utilisateurs
- **Explainable AI :** chaque anomalie accompagnée de son score de risque et sa justification

DÉPLOIEMENT ····· **Complexité : TRÈS FAIBLE**

En rupture avec les approches traditionnelles fondées sur l'échantillonnage, les solutions benchmarkées au Q1 2026 pour la troisième ligne de défense marquent un tournant dans les pratiques d'audit : analyse exhaustive des populations de données, monitoring continu des contrôles, automatisation des tests et génération assistée des rapports par IA.

CAS D'USAGE

CAS 1 — DÉTECTION CONTINUE DES FRAUDES ET ANOMALIES

- **Technologies utilisées :** Rule-based (120 tests auto), ML statistique, connecteurs SAP/achats, alerting temps réel
- **Contexte :** L'Inspection Générale testait 5-10% des transactions — fraudes et erreurs de contrôle passaient inaperçues entre deux missions
- **Action :** Déploiement Diligent HighBond CCM connecté aux systèmes comptables et achats. 120 tests s'exécutent chaque nuit sur 100% des transactions, avec remontée en temps réel aux auditeurs
- **Résultat :** Couverture totale des transactions, 3 cas de fraude interne détectés dès la première année (invisibles en échantillonnage), délai de détection réduit

CAS 2 — AUTOMATISATION DES TESTS D'AUDIT

- **Technologies :** Rule-based (tests continus), ML non supervisé (scoring anomalies), automatisation plan d'audit
- **Contexte :** 12 auditeurs pour 200+ agences, certaines n'étaient auditées que tous les 3-4 ans
- **Action :** Déploiement HighBond avec tests continus sur opérations de caisse, ouvertures de compte et remises de chèques. Les agences présentant des anomalies sont automatiquement priorisées dans le plan d'audit
- **Résultat :** Couverture de risque 100% en continu, plan d'audit risk-based, 2 situations à risque identifiées dans des agences non planifiées

POINTS FORTS & AVANTAGES

- 500+ tests préconfigurés prêts à l'emploi (pas de développement)
- **CCM :** passage des tests annuels aux tests continus en temps réel
- Détection anomalies ML sur 100% des transactions (vs 5-10% en échantillonnage)
- **Generative AI :** rédaction automatique des rapports d'audit
- Leader Gartner Continuous Audit 2024

DÉLAIS — Tests préconfigurés : 4-8 semaines — CCM full custom : 3-5 mois

CAS D'USAGE

CAS 1 — DÉTECTION SAISIES MANUELLES ANORMALES

- **Technologies utilisées :** ML supervisé (scoring écritures), ML non supervisé (détection outliers), connecteur SAP GL, Explainable AI
- **Filiale :** Inspection Générale (audit des processus comptables groupe)
- **Contexte :** L'audit des journaux comptables représentait 50M+ d'écritures par trimestre. L'équipe d'audit ne pouvait analyser que 2% des écritures via échantillonnage, laissant 98% non testées. Les saisies manuelles hors workflow (risque d'erreur ou de fraude) n'étaient pas systématiquement identifiées
- **Action :** Déploiement MindBridge AI Auditor avec connexion au GL SAP. Analyse de 100% des écritures comptables avec scoring ML. Les 200 écritures les plus risquées sont présentées aux auditeurs chaque semaine avec leur justification
- **Résultat :** Couverture d'audit 100% des écritures, 12 saisies manuelles anormales identifiées sur le trimestre (dont 2 ayant conduit à des corrections significatives), temps de préparation audit GL réduit de 3 semaines à 4 jours.

CAS 2 — DÉTECTION FRAUDE COMPTABLE INTERNE

- **Technologies utilisées :** ML non supervisé (patterns fraude), Rule-based (indicateurs comportementaux), scoring risque automatisé
- **Contexte :** L'entité cherchait à identifier les patterns de fraude comptable interne (saisies en dehors des heures ouvrées, comptes de passage utilisés anormalement, montants ronds suspects) sur un volume de données trop important pour une revue manuelle
- **Action :** Utilisation des 25 indicateurs de fraude MindBridge sur le journal comptable. Analyse mensuelle automatique avec rapport des exceptions classées par score de risque
- **Résultat :** 4 cas d'irrégularités comptables identifiés en 6 mois (vs 0 sur la même période avec les méthodes traditionnelles), dont 1 cas de détournement confirmé

POINTS FORTS & AVANTAGES

- Analyse 100% des écritures (vs échantillonnage traditionnel)
- Détection anomalies sur des patterns invisibles à l'œil humain
- Requêtes en langage naturel : pas besoin de compétences SQL
- Journal Entry Testing certifié Big 4 (EY, Deloitte utilisateurs)
- Réduction 70% du temps de préparation de l'audit des comptes
- **Déploiement très rapide :** 2-3 semaines

DÉLAIS — Premier audit opérationnel : 2-3 semaines — Intégration GL complète : 1 mois

05.3. LOD3

L'AUDIT DU FUTUR : COMMENT L'IA TRANSFORME LA 3E LIGNE DE DEFENSE

AUTOMATISATION DES TESTS D'AUDIT

IDEA (CASEWARE) (SPÉCIALISTE ANALYSE DONNÉES AUDIT)

POSITIONNEMENT MARCHÉ : SPÉCIALISTE AUDIT DATA

DESCRIPTION & FONCTIONNALITÉS CLÉS

Logiciel d'analyse de données dédié aux auditeurs internes et externes, utilisé par les Big 4 et les grandes directions d'audit internes mondiales.

- **IDEA Data Analysis :** analyse exhaustive des populations de données d'audit (100% des transactions)
- **100+ tests d'audit préconfigurés :** doublons, lacunes, transactions hors limite, Benford's Law
- **Benford's Law Analysis :** détection de fraude par analyse statistique des chiffres de tête
- **Stratification & Aging :** analyse de vieillissement des créances, provisions, stocks
- **Fuzzy Matching :** détection de doublons malgré variations de saisie (fournisseurs, clients)
- **Scripting IDEA :** automatisation des procédures d'audit récurrentes
- **Export vers TeamMate+ / autres outils :** intégration dossiers de travail
- **SmartAnalyzer :** analyse automatique des populations avec rapport d'exceptions

TECHNOLOGIE CLÉ UTILISÉE

- Statistical analysis avancée pour tests d'audit (loi de Benford, chi-2, régression)
- Fuzzy matching ML pour détection de doublons
- **Anomaly detection :** algorithmes statistiques pour transactions hors normes
- **Sampling intelligent :** sélection d'échantillons d'audit statistiquement représentatifs
- Rules engine pour tests de contrôle déterministes
- Scripting automatisation (langage propriétaire IDEA)
- **Benford's Law :** analyse statistique pour détection de fraude

DÉPLOIEMENT ····· **Complexité : TRÈS FAIBLE**

ROBOTISATION ET INTELLIGENCE ARTIFICIELLE DES PROCÉDURES D'AUDIT

CAS D'USAGE

CAS 1 — DÉTECTION DES FRAUDES ET ERREURS DE FACTURATION GRÂCE À L'ANALYSE DES DONNÉES

- **Technologies utilisées :** Rule-based (scripts fractionnement/seuils), Fuzzy matching ML (doublons factures), automatisation mensuelle
- **Entité :** Direction de l'Audit Interne
- **Contexte :** La DAI auditait le processus achats de ses filiales avec des tests manuels sur des échantillons. Les risques de fractionnement de commandes pour contourner les seuils d'approbation et les doublons de factures n'étaient pas systématiquement détectés
- **Action :** Déploiement IDEA avec scripts automatisés pour 3 tests clés : détection fractionnement (commandes inférieures au seuil sur le même fournisseur dans les 30 jours), doublons de factures (fuzzy matching sur montant + fournisseur + date), et transactions hors délégation. Scripts exécutés à chaque clôture mensuelle
- **Résultat :** 12 cas de fractionnement identifiés sur 2 exercices (dont 3 intentionnels), €340k de doublons de factures récupérés, tests mensuels sans ressources supplémentaires

CAS 2 — ANALYSE EXHAUSTIVE DES DONNÉES ET DÉTECTION ANOMALIES RH PAR ANALYTICS AVANCÉS

- **Technologies utilisées :** Benford's Law (détection manipulation), Rule-based (comparaison référentiel RH), stratification statistique
- **Contexte :** La DAI devait tester la fiabilité de la paie sur 8 000 salariés en identifiant les anomalies (paies fantômes, augmentations non autorisées, absences non décomptées)
- **Action :** Utilisation IDEA pour analyse exhaustive de la population de paie. Tests Benford's Law sur les montants de paie (détection de manipulation), comparaison avec le référentiel RH pour identifier les écarts, stratification par catégorie et ancienneté
- **Résultat :** 3 anomalies significatives détectées (dont 1 salarié fantôme), analyse 100% de la population vs 10% en échantillonnage, temps d'analyse réduit de 3 semaines à 3 jours

POINTS FORTS & AVANTAGES

- Standard des Big 4 pour l'analyse de données d'audit
- 100+ tests préconfigurés sans développement
- **Benford's Law :** détection fraude reconnue par les régulateurs
- Traite des fichiers de millions de lignes sans ralentissement
- Formation certifiante reconnue IIA
- Tarification accessible pour petites DAI

DÉLAIS · Formation et premiers tests : 1-2 semaines · Scripts récurrents : 1-2 mois

05.3. LOD3

L'AUDIT DU FUTUR : COMMENT L'IA TRANSFORME LA 3E LIGNE DE DEFENSE

GESTION DU PLAN D'AUDIT & DOCUMENTATION

AUDITBOARD (AVEC IA GÉNÉRATIVE OPENAI INTÉGRÉE)

POSITIONNEMENT MARCHÉ : LEADER

DESCRIPTION & FONCTIONNALITÉS CLÉS

AuditBoard est une plateforme cloud de gestion de l'audit interne, des risques, de la conformité et des contrôles utilisée par les grandes entreprises et institutions financières. Elle centralise les activités d'audit, de gestion des risques et de contrôle interne dans un environnement unique afin d'améliorer la gouvernance et la transparence.

La solution intègre désormais une IA générative basée sur OpenAI pour automatiser la documentation, l'analyse des risques et la préparation des travaux d'audit. Elle aide les équipes à produire plus rapidement des analyses, synthèses et plans d'audit tout en améliorant la qualité et la cohérence des contrôles.

TECHNOLOGIE CLÉ UTILISÉE

- **Cloud / SaaS :** plateforme entièrement cloud pour centraliser audits, risques et contrôles en temps réel
- **IA générative (OpenAI) :** génération assistée de rapports d'audit, synthèses de risques et documentation
- **Automatisation des workflows :** moteurs d'automatisation pour collecte de preuves, validations et suivi des actions
- **Data analytics & dashboards :** analyse des données de contrôle et tableaux de bord en temps réel
- **APIs & intégrations systèmes :** connexion aux outils internes (ERP, GRC, finance, IT)
- **Sécurité & gestion des accès :** contrôle des accès, traçabilité et conformité aux standards de sécurité

DÉPLOIEMENT ····· **Complexité : MODÉRÉE**

PLANIFICATION, DOSSIERS DE TRAVAIL ET REPORTING COMITÉ D'AUDIT

CAS D'USAGE

CAS 1 — ANALYSE AUTOMATIQUE D'UN GRAND VOLUME DE TRANSACTIONS ET D'ACCÈS UTILISATEURS

- **Technologies utilisées :** ML non supervisé (analyse transactions à grande échelle), Rule-based (accès utilisateurs), automatisation reporting
- **Entité :** Fonction audit interne confrontée à un volume important de données et d'opérations
- **Contexte :** Analyses d'audit réalisées principalement avec des outils manuels et échantillonnage limité ; Difficulté à analyser de grandes populations de transactions et de rôles utilisateurs ; Besoin d'améliorer la couverture d'audit et la rapidité d'analyse des données
- **Solution déployée :** Mise en place de AuditBoard Analytics ; Automatisation de l'analyse des données d'audit et des tests ; Analyse étendue des transactions et des accès utilisateurs à grande échelle
- **Bénéfices observés :** Capacité d'analyse passée d'environ 1 300 à 50 000 transactions ; Audit des accès étendu de 400 à 96 000 rôles utilisateurs ; Analyses et rapports d'audit produits plus rapidement ; Meilleure couverture des risques grâce à l'analyse complète des données

CAS 2 — TRANSFORMATION AUDIT INTERNE GROUPE VIA IA GÉNÉRATIVE, ANALYTICS EXHAUSTIF & RISK MAPPING TEMPS RÉEL

- **Technologies utilisées :** IA Générative (rédaction constats format IIA), ML supervisé (analytics 100% transactionnel), Rule-based (CrossComply multi-référentiels), cartographie dynamique des risques
- **Contexte & Problématique :** Direction de l'Audit Interne d'une banque systémique soumise à une forte pression réglementaire (BCE, Bâle III/IV, RGPD, IIA)
- **Défis Majeurs :** Fragmentation des outils : Usage intensif d'Excel/Word freinant la collaboration inter-pays et la traçabilité ; Inefficacité rédactionnelle : Production manuelle des rapports chronophage, source d'incohérences entre les équipes ; Limites méthodologiques : Tests basés sur l'échantillonnage partiel, laissant passer des risques transactionnels ; Manque de visibilité : Reporting au Comité d'Audit statique et déconnecté du temps réel
- **Solution Déployée :** Produit : Plateforme AuditBoard (Cloud sécurisé); Modules Clés & Technologies : OpsAudit avec IA Générative (Analyse automatique des papiers de travail pour rédiger les constats (format IIA) et harmoniser le style), AuditBoard Analytics (Analyse de 100% des données transactionnelles (vs échantillonnage) pour détecter anomalies et doublons), RiskOversight (Cartographie dynamique des risques connectée au plan d'audit), CrossComply (Gestion centralisée de la conformité multi-référentiels (Bâle, RGPD))
- **Bénéfices Observés :** Productivité Rédactionnelle : Gain de temps de 55% sur la rédaction des rapports (passage de 6-8 jours à 2-3 jours) ; Qualité d'Audit : Passage d'un contrôle par échantillonnage à une analyse exhaustive (100%) des populations de données ; Standardisation : Homogénéité totale des rapports produits entre les différentes entités géographiques ; Pilotage Stratégique : Reporting en temps réel au Comité d'Audit, offrant la transparence exigée par la BCE

POINTS FORTS & AVANTAGES

- **IA Générative (OpenAI) intégrée :** rédaction automatique des constats et rapports d'audit
- Gain de 55% sur le temps de rédaction des rapports (de 6-8 jours à 2-3 jours)
- Analyse exhaustive de 100% des transactions vs échantillonnage partiel
- **Couverture étendue :** de 1 300 à 50 000 transactions analysées, de 400 à 96 000 rôles utilisateurs
- Cartographie dynamique des risques connectée en temps réel au plan d'audit
- Conformité multi-référentiels centralisée (Bâle, RGPD, SOX, IIA)
- **Déploiement SaaS rapide :** 6 à 12 semaines pour un périmètre audit interne standard
- **Plateforme unifiée :** audit, risques et conformité dans un seul environnement collaboratif

DÉLAIS · Déploiement standard : 6-12 semaines · Multi-modules : 3-6 mois · Grand groupe avec ERP : + 6 mois

06.

CAS D'USAGES NEXIALOG

Finance Innovation

NEXIALOG CONSULTING

CAS D'USAGE NEXIALOG CONSULTING : IA & MODÉLISATION DU RISQUE CYBER

Dans le cadre d'un mémoire d'actuariat sur la modélisation de la sévérité du risque cyber, Nexialog a exploré l'utilisation de l'intelligence artificielle générative pour pallier la rareté des données de sinistres graves et améliorer la précision des modèles de détection.

CONTEXTE ET DÉFIS

La cyberassurance se caractérise par une asymétrie extrême des données : 99% des sinistres déclarés sont attritionnels avec un impact financier limité, tandis que 1% concentrent l'essentiel des pertes. Cette distribution fortement déséquilibrée pose un défi majeur aux actuaires et data scientists.

Les modèles d'apprentissage machine entraînés sur ces données reproduisent naturellement le biais majoritaire. Ils excellent à identifier les sinistres courants mais peinent à détecter les événements rares mais critiques, précisément ceux qui déterminent la rentabilité du portefeuille. L'accumulation de données historiques sur les sinistres graves prend des années, voire des décennies, alors que les besoins de tarification et de provisionnement sont immédiats. Les bases de données publiques comme Privacy Rights Clearinghouse, bien que riches en volume, contiennent une majorité écrasante de cas légers qui noient les signaux faibles des sinistres extrêmes.

L'émergence des modèles de langage génératifs comme GPT offre une piste prometteuse : générer artificiellement des descriptions de sinistres graves pour rééquilibrer les jeux d'entraînement et améliorer la capacité prédictive des modèles.

SOLUTION DÉPLOYÉE

Nexialog a intégré l'IA générative dans une approche méthodologique rigoureuse. La génération contrôlée de sinistres synthétiques s'appuie sur GPT-5 pour créer des descriptions textuelles de sinistres cyber graves, calibrées sur les caractéristiques observées dans les cas réels extrêmes : volume de données compromises, secteurs touchés, mécanismes d'attaque. L'enrichissement cible spécifiquement les percentiles les plus élevés de sévérité, là où la rareté des observations réelles pénalise le plus les modèles.

Chaque sinistre généré fait l'objet d'une validation de cohérence pour vérifier qu'il respecte les distributions statistiques observées et les logiques métier du risque cyber. L'entraînement combine ensuite données réelles, données synthétiques enrichies et règles expertes, notamment des expressions régulières pour détecter les mentions numériques explicites dans les descriptions textuelles.

BÉNÉFICES OBSERVÉS

L'intégration de l'IA générative a permis d'améliorer la détection des sinistres graves en réduisant le biais attritional qui affectait les modèles antérieurs. Le cycle de développement s'en trouve accéléré : la capacité à enrichir rapidement les bases d'entraînement évite d'attendre l'accumulation de nouvelles observations réelles sur plusieurs années.

Cette approche offre également une flexibilité de calibrage précieuse. Il devient possible de générer des scénarios de stress spécifiques — attaques sectorielles, ransomwares de nouvelle génération — pour tester la robustesse des modèles face à des menaces émergentes. Le risque de faux négatifs critiques diminue : les sinistres qui auraient échappé aux modèles entraînés uniquement sur données réelles déséquilibrées sont désormais mieux identifiés.

ENSEIGNEMENT CLÉ

L'IA générative constitue un outil puissant pour traiter les problèmes de données asymétriques, mais son efficacité dépend d'un cadrage méthodologique strict. Les travaux menés ont démontré qu'un enrichissement synthétique bien calibré améliore la détection des sinistres graves. Mal paramétré, il peut au contraire aggraver les biais existants en renforçant les patterns majoritaires au détriment des cas rares.

L'IA générative ne remplace pas l'expertise actuarielle. Elle l'augmente. La génération de sinistres synthétiques exige une validation rigoureuse par des experts métier pour garantir la cohérence des scénarios produits. L'interprétation des résultats nécessite un jugement humain pour distinguer les gains réels de détection des artefacts statistiques introduits par les données synthétiques.

Cette approche se positionne comme un outil de maturité pour la deuxième ligne de défense. Elle permet aux fonctions Risques et Actuariat d'anticiper les scénarios extrêmes, d'enrichir leurs analyses de provisionnement et de mieux challenger les modèles opérationnels de tarification déployés par la première ligne. L'IA générative ouvre ainsi la voie à une gestion plus proactive du risque cyber dans un contexte où la sévérité reste le principal angle mort des dispositifs de pilotage.

CAS D'USAGE NEXIALOG CONSULTING : VEILLE RÉGLEMENTAIRE & MAPPING RÉGLEMENTAIRE

CONTEXTE ET DÉFIS

Les institutions financières font face à une accélération sans précédent (DORA, Bâle IV, CRR3, directives LCB-FT..)

Le principal défi n'est plus seulement la compréhension des textes, mais leur intégration opérationnelle rapide et traçable dans le dispositif existant. Dans la pratique, le mapping réglementaire reste largement manuel, chronophage et dépend fortement de l'interprétation individuelle. Partant de ce constat, nous avons conçu un Agent IA spécialisé, testé sur un environnement simulé incluant un corpus de données.

SOLUTION DÉPLOYÉE

Nous avons développé un agent IA dédié à la veille réglementaire et à l'automatisation de mapping, testé sur des données simulées.

L'agent opère en trois couches successives :

1. VEILLE & EXTRACTION RÉGLEMENTAIRE

- Détection automatique des nouvelles publications
- Extraction structurée des exigences clés
- Classification par thématique : crédit, LCB-FT, gouvernance, reporting, IT/cyber, etc.
- Génération d'une synthèse exécutive : obligations nouvelles ou modifiées, échéances, niveau de criticité estimé

2. MAPPING DYNAMIQUE RÉGLEMENTATION ↔ RISQUES ↔ CONTRÔLES (INNOVATION CENTRALE)

- Analyse sémantique du référentiel de contrôle existant
- Rapprochement automatique exigences réglementaires ↔ contrôles en place
- Identification des gaps
- Piste d'audit pour les superviseurs

3. MISE À JOUR ASSISTÉE DU DISPOSITIF

- Proposition de mise à jour des matrices de contrôle
- Suggestions de nouveaux contrôles
- Documentation des justifications
- Validation humaine systématique : l'agent IA propose, l'expert décide

BÉNÉFICES OBSERVÉS

- Une réduction du temps de veille et d'analyse réglementaire
- Une traçabilité renforcée des correspondances réglementaires
- Une capacité d'anticipation des risques de non-conformité
- Un maintien du contrôle humain sur toutes les décisions

ENSEIGNEMENT CLÉ

- L'automatisation du mapping réglementaire est techniquement réalisable
- La valeur ne réside pas uniquement dans la génération de synthèses de textes, mais dans la capacité à relier dynamiquement la réglementation au dispositif de contrôle.
- L'agent est paramétrable selon le périmètre de l'établissement, son référentiel de contrôles et ses sources réglementaires prioritaires

COIN EXPERT

Hugo
RAPIOR

Responsable de programme R&D et du Lab Cyber, Nexialog Consulting

L'INTELLIGENCE ARTIFICIELLE ET LE RISQUE CYBER : QUAND LA SOLUTION DEVIENT AUSSI LA MENACE

Pour la septième année consécutive depuis 2019, le risque cyber occupe la première place de la cartographie prospective de France Assureurs. Cette permanence au sommet ne traduit pas une stagnation du phénomène. Elle révèle au contraire une mutation profonde de sa nature. Les établissements financiers maîtrisent désormais mieux la fréquence des incidents grâce à leurs investissements massifs en cybersécurité. Mais la sévérité potentielle de ces attaques reste totalement imprévisible et continue de progresser.

Cette imprévisibilité croissante trouve son origine dans l'irruption de l'Intelligence Artificielle au cœur de l'écosystème cyber. L'IA joue aujourd'hui un double rôle paradoxal : elle constitue à la fois l'outil le plus prometteur pour détecter et contrer les cyberattaques, et simultanément le vecteur d'amplification des menaces les plus sophistiquées. Les établissements financiers font ainsi face à un défi inédit : comment se protéger d'un risque dont la technologie de défense peut elle-même devenir une vulnérabilité ?

I. LES NOUVELLES MENACES CYBER PORTÉES PAR L'IA

L'IA révolutionne les capacités offensives des attaquants. Trois grandes familles de menaces émergent de cette transformation.

La manipulation des systèmes de détection, aussi appelées attaques adversariales, consiste à tromper les algorithmes en ajustant subtilement les données d'entrée. Un fraudeur peut ainsi apprendre progressivement à contourner un système de scoring en modifiant son comportement jusqu'à ce qu'il soit classé comme « légitime » par le modèle. L'article 15 du règlement européen sur l'IA exige que les fournisseurs de systèmes à haut risque testent la résistance de leurs modèles face à ce type d'attaques, une exigence qui formalise une pratique encore peu répandue dans le secteur.

L'empoisonnement des données d'entraînement vise à corrompre les bases de données utilisées pour construire les modèles d'IA. En injectant des exemples malveillants, un attaquant peut rendre l'IA complice involontaire de la fraude qu'elle est censée détecter.

Les escroqueries ultra-personnalisées exploitent quant à elles les capacités génératives des LLM pour produire en masse des contenus parfaitement contextualisés. Là où un attaquant devait auparavant rédiger manuellement quelques dizaines de messages ciblés, il peut désormais générer des milliers de variantes personnalisées en quelques secondes.

Un constat s'impose : les attaquants adoptent l'IA plus rapidement que les défenseurs ne sécurisent leurs propres systèmes. Cette asymétrie temporelle crée un décalage stratégique croissant. Si ce phénomène n'est pas nouveau dans le domaine de la cybersécurité, où les attaquants ont toujours innové plus rapidement que les défenseurs, l'IA en change radicalement l'ampleur et la vitesse. Les travaux de recherche menés à Nexialog, notamment dans le cadre du mémoire d'actuariat de Franck Dountio que j'ai encadré, montrent que même les modèles de détection les plus performants peinent à identifier les sinistres cyber les plus graves. Cette limite

souligne que les angles morts des défenseurs sont déjà connus et exploités.

La convergence entre cyber, IA et géopolitique ajoute une dimension supplémentaire. Une part importante des institutions financières françaises utilisent des solutions d'IA hébergées sur des infrastructures cloud non européennes. Cette dépendance crée des vulnérabilités juridiques, avec des législations extraterritoriales comme le Cloud Act américain permettant l'accès aux données même stockées en Europe. Les attaques orchestrées ou financées par des États combinent désormais sophistication technique et objectifs géopolitiques : espionnage industriel systématique, corruption de modèles critiques, utilisation de vidéos et audios truqués (deepfakes) pour déstabiliser les marchés. La question de la souveraineté technologique est ainsi devenue un enjeu prudentiel majeur, même si ni l'IA Act ni DORA n'imposent explicitement de privilégier des solutions européennes.

II. COMMENT L'IA RENFORCE LA DÉTECTION ET LA MAÎTRISE DU RISQUE CYBER

Malgré les menaces qu'elle génère, l'IA demeure l'outil le plus efficace pour contrer les cyberattaques modernes. Les modèles d'apprentissage machine permettent d'analyser en continu des millions de flux de données et d'identifier des patterns anormaux invisibles à l'œil humain. Cette capacité transforme radicalement les dispositifs de cybersécurité.

Les travaux menés dans le cadre du mémoire d'actuariat de Franck Dountio, dont les résultats ont été présentés lors de notre atelier sur le risque cyber au sein de l'événement 100% Actuaires – Data Science, illustrent concrètement comment l'IA peut renforcer la détection des sinistres cyber graves. Une leçon majeure émerge de ces recherches : l'IA seule ne suffit pas. Les approches les plus performantes combinent la puissance de calcul des modèles avec l'expertise humaine.

Notre premier cas d'usage porte sur l'analyse automatisée des rapports d'incidents cyber. En associant des modèles d'apprentissage profond avec des règles expertes — notamment la détection de mentions explicites de volumes de données compromises dans les descriptions textuelles — les performances de détection des sinistres graves augmentent significativement. Cette approche hybride compense les angles morts des modèles purement statistiques, qui peinent à interpréter certaines informations quantitatives pourtant déterminantes pour évaluer la sévérité. Les établissements qui articulent efficacement outils IA et expertise métier obtiennent ainsi les meilleurs résultats en termes de ratio sinistres sur primes.

Notre second cas d'usage concerne la génération synthétique de données pour l'entraînement des modèles. Un défi majeur de la cyberassurance réside dans le fort déséquilibre des données : 99% des sinistres sont attritionnels avec un faible impact, tandis que 1% concentrent l'essentiel des pertes. Cette asymétrie rend difficile l'entraînement de modèles capables de détecter les événements rares mais critiques. Les modèles génératifs comme GPT permettent de créer artificiellement des descriptions de sinistres graves pour enrichir les bases d'apprentissage. Ces travaux montrent que cette approche améliore la détection à condition d'être méthodologiquement encadrée : un enrichissement mal calibré peut au contraire aggraver les biais existants en renforçant les patterns majoritaires au détriment des cas rares.

Notre analyse du rapport LUCY 2025 sur le marché de la cyberassurance confirme l'aggravation de la sévérité des sinistres cyber et la nécessité de renforcer les dispositifs de détection. Au-delà de ces cas d'usage spécifiques, l'IA transforme également la réponse aux incidents. Les systèmes d'automatisation intelligente réduisent le délai entre détection et remédiation de plusieurs heures à quelques minutes, limitant ainsi l'exposition. Cette rapidité devient cruciale face à des attaques qui progressent elles aussi de plus en plus vite grâce aux mêmes technologies.

III. LE RÔLE CLÉ DE LA DEUXIÈME LIGNE DE DÉFENSE DANS LE CONTRÔLE DES SYSTÈMES IA

La fonction Risques, deuxième ligne de défense, se trouve au cœur de cette transformation. Son rôle traditionnel de contrôle et de challenge s'étend désormais à une dimension nouvelle : valider que les systèmes d'IA déployés par l'opérationnel pour gérer le risque cyber ne deviennent pas eux-mêmes des sources de vulnérabilité. Cette mission impose de développer des compétences hybrides et de nouveaux processus de contrôle.

Le premier enjeu consiste à challenger les décisions de déploiement de systèmes d'IA par la première ligne. Lorsqu'une direction métier souhaite déployer un modèle de détection de fraude ou un système d'analyse comportementale, la LOD2 doit évaluer non seulement sa performance technique, mais aussi sa robustesse face aux menaces cyber spécifiques à l'IA. Cette évaluation implique de vérifier que des tests adversariaux ont été réalisés, que la qualité des données d'entraînement est documentée et traçable, et que des mécanismes de détection de corruption ou de dérive sont prévus. L'article 15 de l'IA Act rend ces tests obligatoires

pour les systèmes à haut risque, mais la LOD2 doit aller au-delà de la simple conformité formelle pour s'assurer de leur efficacité réelle.

Le deuxième enjeu porte sur le suivi continu des systèmes en production. La LOD2 doit définir et monitorer des indicateurs clés de risque spécifiques aux systèmes IA-Cyber : taux de fausses alertes et de faux négatifs, temps de détection des incidents, évolution des patterns de décision des modèles, incidents de performance inexpliqués qui pourraient signaler une compromission. Ces KRI permettent de détecter précocement les dérives et les anomalies qui échappent souvent aux équipes opérationnelles focalisées sur les métriques de performance business. Le règlement IA Act impose par son article 72 un suivi post-commercialisation des systèmes à haut risque, donnant ainsi une base réglementaire à cette mission de la LOD2.

Le troisième enjeu concerne la validation de la gouvernance des fournisseurs d'IA tiers. Lorsque l'établissement s'appuie sur des solutions externes, la LOD2 doit s'assurer que les contrats incluent les clauses spécifiques exigées par l'article 16 de l'IA Act : droit d'audit des systèmes critiques, obligations de documentation, notification rapide des incidents, clause de réversibilité. Cette due diligence s'étend aux enjeux de souveraineté : la LOD2 doit documenter les risques juridiques et géopolitiques associés à l'hébergement des données et des modèles hors Europe, et challenger les arbitrages entre performance technique et maîtrise des risques.

Cette montée en compétence de la LOD2 ne peut se faire isolément. Elle nécessite une collaboration étroite avec les équipes Data Science pour comprendre les architectures techniques, avec le RSSI pour intégrer les menaces cyber émergentes, et avec les équipes Conformité pour articuler les exigences de l'IA Act, de DORA et du RGPD.

IV. ACCOMPAGNER LES ÉTABLISSEMENTS : MÉTHODOLOGIE ET BONNES PRATIQUES

« Une approche efficace pour accompagner les établissements financiers consiste à articuler la mise en conformité autour de quatre axes complémentaires, permettant de prioriser les actions selon leur impact et leur faisabilité. »

La première étape consiste à établir un diagnostic d'exposition. Il s'agit d'identifier l'ensemble des systèmes d'IA déployés ou en développement qui traitent des données sensibles ou pilotent des processus critiques. Cette cartographie doit alimenter le registre des systèmes d'IA imposé par l'article 71 de l'IA Act pour les systèmes à haut risque. Elle permet de prioriser les efforts de sécurisation sur les actifs les plus exposés. La plupart des établissements sous-estiment le nombre de systèmes d'IA qu'ils utilisent réellement, en particulier les solutions intégrées dans des produits tiers, une situation qui complique la mise en conformité avec les obligations de cartographie.

La deuxième étape vise à structurer les responsabilités et les processus de validation. Qui valide le déploiement d'un nouveau modèle d'IA ? Qui contrôle sa robustesse cyber ? Qui décide de sa mise hors service en cas de dérive détectée ? Ces questions, apparemment simples, restent souvent sans réponse claire dans les organisations. L'article 4 de l'IA Act impose une obligation de maîtrise qui nécessite de former les équipes concernées et de formaliser les circuits de décision. Cette structuration doit articuler les rôles des trois lignes de défense, même si les textes réglementaires ne prescrivent pas explicitement cette organisation. Les superviseurs, notamment l'ACPR et la BCE, encouragent cette coordination transverse dans leurs guidelines et travaux de supervision.

La troisième étape porte sur la mise en place des contrôles techniques et documentaires. Les tests adversariaux, l'analyse de la qualité des données, le monitoring des dérives, la conservation des preuves de conformité pendant dix ans comme l'exigent les articles 18 et 19 de l'IA Act : autant d'obligations qui nécessitent des investissements en compétences et en outils. Les travaux menés par Nexialog sur la conformité à l'IA Act, notamment notre analyse du cadre réglementaire et du GPAI Code of Practice, précisent ces exigences et leurs implications opérationnelles pour les établissements financiers. L'accompagnement consiste ici à définir le niveau de contrôle proportionné au niveau de risque, à identifier les solutions techniques adaptées au contexte de l'établissement, et à former les équipes aux nouveaux processus.

La quatrième étape concerne l'intégration des enjeux de souveraineté dans les décisions technologiques. Si ni l'IA Act ni DORA n'imposent explicitement de privilégier des solutions européennes, les établissements les plus matures intègrent désormais ces critères dans leurs choix d'architecture. Cette démarche s'appuie sur une analyse approfondie des fournisseurs : localisation des données et des traitements, juridiction applicable, clauses de réversibilité, scénarios de coupure d'accès. Le règlement DORA renforce ces exigences en imposant des tests de résilience opérationnelle incluant explicitement des scénarios de défaillance des prestataires tiers critiques.

QUESTIONS CLÉS POUR ÉVALUER VOTRE MATURITÉ

Six questions permettent d'évaluer rapidement le niveau de maturité de votre gouvernance IA-Cyber.

1. Disposez-vous d'un registre complet de vos systèmes d'IA avec leur classification par niveau de risque, conformément à l'article 71 de l'IA Act ?
2. Avez-vous réalisé des évaluations d'impact sur les droits fondamentaux pour vos systèmes à haut risque, comme l'exige l'article 27 ?
3. Testez-vous régulièrement la robustesse cyber de vos modèles face aux manipulations et corruptions, en application de l'article 15 ?
4. Vos contrats avec les fournisseurs d'IA incluent-ils les clauses spécifiques exigées par l'article 16, notamment le droit d'audit ?
5. Disposez-vous d'un processus permettant de signaler un incident grave IA aux autorités compétentes dans les délais prescrits (2 à 15 jours selon la gravité), conformément à l'article 73 ?
6. Vos équipes ont-elles été formées aux risques de l'IA, en application de l'obligation de maîtrise de l'article 4 ?

V. PERSPECTIVES : TROIS CERTITUDES ET UNE OPPORTUNITÉ

Trois certitudes se dégagent pour les années à venir :

- La pression réglementaire va s'intensifier : au-delà de DORA et de l'IA Act, les régulateurs nationaux renforceront leurs contrôles et imposeront des stress tests incluant des scénarios de coupure d'accès aux infrastructures critiques.
- L'asymétrie entre attaquants et défenseurs persistera : les cybercriminels continueront d'innover plus rapidement, imposant une transformation profonde des organisations et des compétences.
- Enfin, la fragmentation géopolitique s'accentuera, obligeant les établissements à naviguer dans un environnement où standards techniques, réglementations et infrastructures divergent entre blocs.

Face à ces certitudes, une opportunité majeure s'ouvre aux établissements qui maîtriseront cette convergence IA-Cyber-Géopolitique. Ils disposeront d'un avantage compétitif triple : confiance client renforcée par la démonstration de leur conformité et de leur résilience, différenciation réglementaire permettant d'influencer l'évolution des pratiques de marché, et capacité à maintenir l'activité face aux chocs technologiques ou géopolitiques. Cette résilience, loin d'être un simple objectif de conformité, devient un levier de création de valeur durable.

LE PARADOXE DE L'IA EN CYBERSÉCURITÉ

Plus les établissements financiers déploient de l'IA pour détecter les cyberattaques, plus ils deviennent dépendants de ces systèmes. Cette dépendance crée de nouvelles vulnérabilités que les attaquants ont rapidement identifiées. L'IA elle-même devient une cible prioritaire : corruption de modèles, manipulation des systèmes de détection, exploitation des biais d'apprentissage. Pour se protéger de ces nouvelles menaces, les établissements déploient encore plus d'IA, créant une boucle auto-renforçante.

Cette dynamique explique pourquoi le risque cyber reste au sommet des préoccupations malgré les investissements massifs en sécurité. Le cyber n'est plus un risque technique périphérique. C'est devenu un enjeu de souveraineté économique où l'IA joue le rôle de catalyseur. Les établissements qui l'ont compris transforment cette contrainte en levier stratégique pour renforcer leur position concurrentielle et leur résilience face aux chocs futurs.

POUR ALLER PLUS LOIN

- Rapport LUCY 2025 : Analyse du marché de la cyberassurance
- GPAI Code of Practice : Guide de conformité IA Act – Analyse Nexialog des obligations réglementaires
- Atelier Risque Cyber – 100 Actuaires × 100 Data Science
- Mémoire d'actuariat de Franck Dountio (2026) : Modélisation de la sévérité du risque cyber en assurance : apports du NLP et de l'IA générative face au déséquilibre des données
- CESIN. Baromètre de la Cybersécurité 2025 – 10 édition. Consulté en octobre 2025.

07.

CONSTRUIRE UNE IA : DEFIS & SOLUTIONS

Finance Innovation

NEXIALOG CONSULTING

La normalisation et l'intégration l'intelligence artificielle (IA) offrent de nombreux avantages :

- Plus d'efficacité
- Des services mieux personnalisés
- Une détection plus fine des anomalies.

Cependant, cette transformation n'est pas sans risques. Il est donc important d'anticiper les enjeux techniques, éthiques et organisationnels

Ce chapitre met l'accent sur les principaux risques liés à l'IA et les leviers pour les maîtriser, en mettant en avant trois défis majeurs (à droite).

Et en proposant des solutions concrètes, appuyées par des exemples issus du secteur bancaire et assurantiel.

Figure 7.1

BIAIS ALGORITHMIQUES

Les biais dans les algorithmes d'IA peuvent fausser les décisions et entraîner des discriminations. C'est un vrai sujet dans des domaines sensibles comme l'octroi de crédit ou la tarification en assurance.

1. DESCRIPTION DU RISQUE

Les biais peuvent provenir de deux sources principales :

- **Biais de données :** Les données historiques reflètent des discriminations passées
- **Biais d'algorithmes :** Les développeurs n'anticipent pas certains effets discriminatoires

LE RISQUE DE DISCRIMINATION INDIRECTE

Au-delà de l'utilisation explicite de variables sensibles (sexe, origine ethnique, orientation politique), l'un des risques majeurs identifiés par l'IA Act européen concerne la reconstitution indirecte de ces informations. Même lorsque ces variables sont explicitement exclues des modèles, les algorithmes de machine learning peuvent les déduire à partir d'autres variables corrélées. Par exemple, des données géographiques ou socio-économiques peuvent permettre d'inférer avec une forte probabilité des caractéristiques protégées, conduisant à des décisions discriminatoires en matière d'assurance, de crédit ou de segmentation client.

UN CAS PARTICULIER : LE BIAIS ATTRITIONNEL

Dans certains domaines comme la cyberassurance, les données présentent une asymétrie extrême qui crée un biais structurel : les modèles peinent à détecter les événements rares mais critiques qui déterminent la rentabilité. Les travaux menés à Nexialog ont démontré qu'une approche hybride, combinant IA et règles expertes, permet de compenser ce type de biais (voir use case p.XX).

RISQUES RÉPUTATIONNELS DES IA PUBLIQUES

L'utilisation d'IA génératives accessibles publiquement (chatbots, réseaux sociaux, outils de communication externe) expose les entreprises à des risques réputationnels importants. Des failles comme la réinitialisation ou le contournement des instructions initiales d'un agent peuvent permettre à des utilisateurs malveillants de lui faire produire des contenus inappropriés ou contraires aux valeurs de l'entreprise, tout en utilisant son identité. Ces vulnérabilités ont déjà causé des incidents réputationnels documentés, notamment lors des premières vagues de déploiement public des grands modèles de langage.

2. EXEMPLE : ALGORITHME DE SCORING BANCAIRE

> *Dans ce cas de scoring de crédit qu'on a vu plus haut dans le livre blanc, l'IA permet d'accélérer et d'améliorer la décision d'octroi. Mais ce même avantage peut devenir un risque : si les données historiques reflètent que les candidats masculins ont été plus fréquemment approuvés que les candidates féminines dans le passé. L'algorithme apprend spontanément à favoriser les hommes, reconduisant ainsi un biais sexiste dans l'attribution des prêts.*

3. SOLUTIONS

TYPE DE BIAIS	ACTION	MÉTHODE
Biais de données	Nettoyer et équilibrer les données d'entraînement. **Garantir leur représentativité et leur qualité (Art. 10 IA Act)**	Analyse de représentativité, sur-échantillonnage, enrichissement par IA générative
Biais d'algorithmes	Tester la performance sur différents groupes. **Tester la robustesse face aux manipulations et corruptions (Art. 15 IA Act), incluant des tests adversariaux**	Tests de parité, audits réguliers. **Approches hybrides combinant IA et règles expertes**
Gouvernance	Mettre en place des comités d'éthique. **Identifier et limiter les mécanismes permettant la reconstitution indirecte de variables sensibles**	Validation humaine, transparence des décisions, **documentation complète du cycle de vie des modèles**

Tableau 7.1

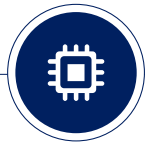
CADRE RÉGLEMENTAIRE

Le règlement européen sur l'IA formalise ces exigences. L'article 10 impose des critères stricts de qualité et de représentativité des données d'entraînement, tandis que l'article 15 rend obligatoires les tests de robustesse, y compris face aux manipulations adversariales, pour tous les systèmes à haut risque. Ces obligations formalisent des pratiques encore en cours de structuration dans le secteur et placent la prévention de la discrimination au cœur de la conformité.

Les organisations doivent donc veiller non seulement à supprimer les variables discriminantes explicites, mais aussi à identifier et limiter les mécanismes permettant leur reconstitution indirecte, afin de prévenir tout biais systémique dans les décisions automatisées.

IMPACT : ***Selon une étude de Gartner, 50% des entreprises reconnaissent avoir rencontré des problèmes de biais dans leurs systèmes d'IA.***

SÉCURITÉ INFORMATIQUE



Les systèmes d'IA traitent données sensibles. Ils peuvent être exposés à différents types d'attaques, ce qui représente un risque important pour la confidentialité et l'intégrité des données

1. DESCRIPTION DU RISQUE

Les principales menaces incluent :

- Attaques adversariales : Manipulation des données d'entrée pour tromper l'algorithme
- Vol de modèles : Extraction de la propriété intellectuelle de l'algorithme
- Empoisonnement de données : Injection de données corrompues pendant l'entraînement

2. EXEMPLE : SYSTÈME DE DÉTECTION DE FRAUDE

> *Une compagnie d'assurance utilise un système d'IA pour détecter les déclarations frauduleuses. Des fraudeurs sophistiqués analysent le comportement du système et apprennent à formuler leurs déclarations de manière à éviter la détection, en modifiant subtilement certains paramètres pour ressembler à des cas légitimes.*

3. SOLUTIONS

TYPE DE MENACE	ACTION	TECHNOLOGIE
Attaques adversariales	Entraînement adversarial et validation robuste	Defensive distillation, détection d'anomalies
Protection des données	Chiffrement et anonymisation	Chiffrement homomorphe, confidentialité différentielle
Surveillance	Monitoring continu et audits de sécurité	SIEM, tests d'intrusion réguliers

Tableau 7.2

RÉGLEMENTATION : ***La directive européenne NIS2 impose des standards de sécurité renforcés pour les institutions financières utilisant l'IA.***

INTÉGRATION AUX SYSTÈMES EXISTANTS

L'intégration de solutions d'IA dans des infrastructures bancaires existantes, souvent basées sur des systèmes legacy, représente un défi technique et organisationnel majeur.

1. DESCRIPTION DU RISQUE

Les défis d'intégration comprennent :

- Incompatibilité technologique : Systèmes legacy incompatibles avec les architectures modernes d'IA
- Qualité des données : Données dispersées, non standardisées ou incomplètes
- Complexité opérationnelle : Coordination entre équipes IT, métiers et data science

2. EXEMPLE : CHATBOT BANCAIRE

Une banque souhaite déployer un chatbot d'IA pour le service client. Le système doit accéder aux données clients stockés dans un mainframe des années 1990, se connecter au système de gestion des comptes, respecter les protocoles de sécurité stricts, et s'intégrer avec le CRM existant. Les formats de données sont hétérogènes et les APIs inexistantes.

3. SOLUTIONS

DÉFI	ACTION	APPROCHE
Systèmes legacy	Créer des APIs et middlewares d'intégration	Architecture microservices, ESB, connecteurs
Qualité des données	Nettoyer et standardiser les données	Data lakes, ETL, gouvernance des données
Déploiement	Approche progressive par phases pilotes	POC, MVP, déploiement itératif

Tableau 7.3

CLÉ DU SUCCÈS : ***L'évaluation préalable des besoins et la formation des équipes sont essentielles pour une intégration réussie.***

VUE D'ENSEMBLE : RISQUES ET SOLUTIONS

RISQUE	IMPACT PRINCIPAL	SOLUTION PRIORITAIRE	RESPONSABILITÉ
Biais algorithmiques	Discrimination, conformité légale	Audits et comités d'éthique	Direction + Data Science
Sécurité informatique	Fuite de données, fraude	Chiffrement et monitoring	RSSI + IT
Intégration système	Échec projet, coûts	Architecture modulaire	DSI + Métiers

Tableau 7.4

En conclusion, l'IA est une vraie opportunité pour la finance, mais elle doit être déployée avec prudence. Pour éviter les dérives, il faut une démarche claire et bien encadrée.

Les trois défis (biais, cybersécurité et intégration aux systèmes existants) peuvent être maîtrisés grâce à une bonne gouvernance et à des contrôles sérieux tout au long du projet

Points clés à retenir :

- La prévention des biais commence dès la conception et nécessite des audits réguliers
- La sécurité doit être intégrée nativement dans les systèmes d'IA, pas ajoutée a posteriori
- L'intégration progressive par phases pilotes limite les risques et facilite l'adoption

Les institutions financières qui investissent dans la formation de leurs équipes, établissent une gouvernance claire et adoptent une approche itérative maximisent leurs chances de succès dans la transformation par l'IA, tout en préservant la confiance de leurs clients et la conformité réglementaire.

08.

VISION 2030 ET SCENARIOS D'EVOLUTION

Finance Innovation

NEXIALOG CONSULTING

RUPTURE STRUCTURELLE, PAS UNE ÉVOLUTION INCRÉMENTALE

Selon nos études, d'ici 2030 l'IA ne sera plus un sujet d'innovation parmi d'autres. Tout indique qu'elle deviendra une infrastructure critique, au même titre que les systèmes financiers, les chaînes d'approvisionnement ou les systèmes d'information stratégiques. Elle influencera directement la manière dont les organisations décident, opèrent et se gouvernent. Ce qui se joue n'a rien d'un ajustement progressif : c'est une rupture structurelle dans les modèles de responsabilité, de contrôle et de gestion.

Nous assistons à un basculement profond : l'IA passe de l'assistance à l'exécution. Là où elle fournissait autrefois analyses et recommandations, elle intervient désormais dans les décisions opérationnelles, l'arbitrage automatisé et, parfois, dans l'activation même des systèmes d'entreprise. Cette évolution recompose entièrement l'architecture du risque : il ne s'agit plus seulement d'évaluer la qualité des résultats produits par l'IA, mais de comprendre la portée de ses actions et les effets qu'elle peut déclencher.

Les analyses prospectives convergent. Les scénarios élaborés par les analystes et les institutions montrent que l'IA sera intégrée dans toutes les chaînes de valeur à l'horizon 2030. Gartner estime qu'elle influencera l'ensemble des métiers de l'informatique, et qu'une part significative des tâches sera automatisée par des systèmes intelligents. Pour les dirigeants, un changement majeur s'impose : l'IA devient un enjeu de gouvernance au plus haut niveau, et ne peut plus être considérée comme un sujet purement technologique ou opérationnel.

UNE REDISTRIBUTION MASSIVE DE LA RESPONSABILITÉ ET DU RISQUE.

La responsabilité ne disparaît pas lorsque des décisions ou des actions sont partiellement automatisées : elle se transforme. Elle se répartit entre les choix de conception, les règles d'utilisation, les données mobilisées, les modèles déployés et les mécanismes de supervision humaine. Chaque étape compte, et chacune porte une part de responsabilité.

Pour les comités exécutifs et les conseils d'administration, l'enjeu est clair. Dans des chaînes de décision hybrides, il devient indispensable de savoir qui est responsable de quoi, de le documenter clairement et d'être en mesure de le démontrer. Sans cela, l'organisation s'expose à des risques juridiques, réglementaires, réputationnels ou opérationnels, des risques parfois diffus, mais qui peuvent devenir systémiques.

Les institutions internationales partagent ce constat. L'OCDE souligne que la gouvernance de l'IA est aujourd'hui l'un des principaux leviers de confiance et de performance durable. Elle met aussi en avant un point critique : le manque de compétences techniques et de leadership numérique reste l'un des obstacles majeurs à une gestion efficace des risques liés à l'IA. Pour les dirigeants, le message est clair : la gouvernance de l'IA ne peut pas être déléguée sans contrôle.

NOUVELLES EXIGENCES DE GOUVERNANCE ET DE PREUVE.

Dans un environnement où les systèmes évoluent en permanence et apprennent à partir des données et où le comportement change avec le temps, les approches traditionnelles de la conformité et du contrôle atteignent leurs limites. L'utilisation d'audits occasionnels et de dispositifs documentaires statiques ne suffit plus comme preuve de gestion des risques. La gouvernance de l'IA, en 2030, repose sur une nouvelle exigence : la capacité à apporter une preuve continue.

Concrètement ''les organisations doivent être pouvoir montrer, à tout moment, quels systèmes d'IA sont utilisés, dans quels cas d'utilisation, avec quelles données, quels modèles et les versions et sous quels contrôles humains et techniques''. Cette exigence transforme la conformité en un dispositif vivant, intégré aux gestions opérationnelles et stratégiques.

Pour les dirigeants, cela implique un changement de posture. La conformité et le contrôle interne ne sont plus seulement des mécanismes de surveillance : ils deviennent des leviers de sécurisation de la stratégie, permettant d'arbitrager lucidement entre l'innovation, la performance et l'exposition au risque.

LES HUMAINS AU CENTRE : UNE RESPONSABILITÉ NON TRANSFÉRABLE

A mesure que l'IA progresse, une tentation persiste, le transfert implicite de responsabilité aux systèmes. D'autre part, les cadres de référence internationaux nous rappellent un principe fondamental selon lequel l'humain demeure responsable.

Les systèmes d'IA peuvent assister, suggérer, exécuter. Mais ils ne porteront jamais la responsabilité finale des décisions prises. Cette responsabilité : éthique, légale, stratégique reste humaine.

A l'horizon 2030, l'enjeu ne sera donc pas de « faire confiance » aux algorithmes, mais de construire un cadre explicite de responsabilité. Cela impose quatre impératifs : garantir une supervision humaine effective, encadrer strictement l'autonomie des systèmes, établir une traçabilité totale des décisions automatisées, et former massivement les acteurs concernés.

MESSAGE CLÉ POUR LES COMITÉS EXÉCUTIFS ET LES CONSEILS D'ADMINISTRATION

A l'horizon 2030, l'IA ne sera pas une option, un choix stratégique, elle sera une réalité structurelle à laquelle toutes les organisations devront s'adapter. Le dilemme pour les dirigeants n'est plus de savoir s'ils doivent adopter l'IA, mais plutôt comment ils décident de la gouverner.

Cette feuille de route propose une trajectoire progressive, réaliste et pilotable qui va au-delà de la logique de l'adoption opportuniste vers une gouvernance stratégique et contrôlée de l'IA. Elle repose sur un principe de base : plus l'IA devient puissante et autonome, plus la responsabilité humaine doit être organisée, documentée et démontrable.

FEUILLE DE ROUTE STRATÉGIQUE 2026-2030

D'ici 2030, l'intelligence artificielle ne sera pas une option, un choix stratégique, elle sera une réalité structurelle à laquelle toutes les organisations devront s'adapter. Le dilemme pour les dirigeants n'est plus de savoir s'ils doivent adopter l'IA, mais plutôt comment ils décident de la gouverner.

Cette feuille de route propose une trajectoire progressive, réaliste et pilotable qui va au-delà de la logique de l'adoption opportuniste vers une gouvernance stratégique et contrôlée de l'IA. Elle repose sur un principe de base : plus l'IA devient puissante et autonome, plus la responsabilité humaine doit être organisée, documentée et démontrable.

Pour réaliser un changement efficace vers un contrôle interne accru, il doit être mis en œuvre en succession :

2026 : RENFORCER LES FONDATIONS

- Assurer une meilleure qualité et gouvernance des données.
- Former les collaborateurs à l'utilisation et aux limites de l'IA.
- Établir des comités éthiques et une supervision des algorithmes

2026-2028 : INDUSTRIALISER LES USAGES

- Déployer des solutions d'automatisation pour les processus à fort volume (reporting, surveillance des transactions).
- Développer des compétences en audit algorithmique et en explicabilité.
- Renforcer la collaboration entre le contrôle interne, l'informatique et les fonctions de risque.

2028-2030 : S'AMÉLIORER ET MAINTENIR UNE SUPERVISION RÉGULIÈRE ET UNE ANALYSE PRÉDICTIVE.

- Incorporer les leçons apprises pour une meilleure gouvernance.
- Établir la fonction de contrôle interne comme un levier stratégique de performance et de confiance.

Cette approche incrémentale permet d'éviter les ruptures et aide à soutenir le changement structurel créé par l'intelligence artificielle.

CONCLUSION

Ce livre blanc a exploré comment l'intelligence artificielle transforme les trois lignes de défense. Du cadre réglementaire de l'IA Act aux cas d'usage concrets déployés dans le secteur financier, en passant par les enjeux de gouvernance des données et les solutions disponibles sur le marché, un constat s'impose : cette transformation est déjà en cours. Elle ne repose pas sur la technologie seule, mais sur un équilibre entre innovation, maîtrise des risques et responsabilité organisée. Si l'IA permet aujourd'hui d'automatiser les contrôles et d'accélérer les décisions, son déploiement ne peut réussir sans des bases solides. La priorité doit désormais porter sur la maturité des fondations.

Dans ce nouvel écosystème, la donnée n'est plus seulement un actif technologique, c'est une responsabilité critique dont la fiabilité conditionne l'entière relation de confiance. Une donnée incorrecte dégrade tous les modèles, même les plus performants. Les organisations qui négligent cet investissement préalable s'exposent à des biais amplifiés et à des décisions inauditables. La gouvernance des données n'est pas une condition préalable parmi d'autres, c'est la condition nécessaire à toute valeur durable.

Les travaux menés par Nexialog illustrent cette exigence. La modélisation de la sévérité cyber par IA générative ou l'analyse du GPAI Code of Practice démontrent qu'il faut hybrider expertise réglementaire et maîtrise technique. Aucun des cas d'usage examinés ne conduit à la conclusion que l'IA supplante le jugement humain. Au contraire : chaque déploiement réussi repose sur le principe que l'IA assiste et fiabilise, mais que la décision finale reste humaine et explicable. Le succès dépend de notre capacité à combiner l'intelligence humaine et artificielle. L'IA libère les équipes des tâches chronophages pour les repositionner sur des analyses à haute valeur ajoutée.

Cette mutation s'accompagne d'un déplacement du risque. Plus les établissements déploient de l'IA, plus ils créent de nouvelles surfaces d'exposition. L'adoption de l'IA ne réduit pas simplement les risques existants, elle en génère de nouveaux : fraudes augmentées par les deepfakes, biais algorithmiques discriminatoires, dépendance à des modèles hébergés hors d'Europe. Maîtriser ses propres modèles d'IA devient un choix stratégique de souveraineté numérique.

Face à cette multiplication des points de vulnérabilité, la régulation devient un impératif stratégique. Plutôt que de subir l'IA Act comme une contrainte, les organisations doivent y voir un levier de résilience. Il structure les fondations d'une « IA de confiance » où seule une gouvernance rigoureuse permet de transformer ces nouveaux risques en un dispositif de contrôle maîtrisé. L'enjeu à l'horizon 2030 n'est plus de tester l'IA, mais de l'ancrer durablement au cœur des dispositifs de contrôle et de supervision.

À mesure que les algorithmes gagnent en autonomie, une tentation persiste : le transfert implicite de responsabilité aux systèmes. Ces systèmes peuvent assister, suggérer, exécuter. Mais ils ne porteront jamais la responsabilité finale des décisions prises. Cette responsabilité reste humaine, qu'elle soit éthique, légale ou stratégique. La supervision humaine devient impérative, l'autonomie des systèmes doit être strictement encadrée, toute décision automatisée tracée, et les acteurs formés massivement.

Les institutions qui réussiront ne seront pas celles qui auront déployé le plus de modèles. Ce seront celles qui auront su bâtir le triptyque données-gouvernance-formation pour faire de l'IA un levier de confiance autant que de performance.

Plus les algorithmes gagnent en autonomie, plus la responsabilité humaine doit être organisée et démontrable. La question n'est donc pas de savoir jusqu'où l'IA peut aller mais jusqu'où nous sommes prêts à organiser notre propre vigilance.

À l'horizon 2030, l'IA sera pleinement intégrée dans les processus opérationnels, risques, finance, conformité et audit. Les institutions devront garantir des systèmes d'IA fiables, traçables, robustes et conformes aux exigences européennes. Grâce à nos expertises complémentaires, nous aidons les organisations à franchir ce cap en combinant technologie, réglementation et transformation des métiers.

Notre pôle Data Consulting sécurise l'intégration de l'IA grâce à une maîtrise complète de la chaîne data : qualité, gouvernance, pipelines, industrialisations des modèles. Avec Finance, Control & Compliance, nous accompagnons la mise en œuvre du cadre réglementaire IA Act, le renforcement de la gouvernance, la supervision et la formalisation des contrôles.

Nos équipes Risk Models & Strategy apportent une expertise sur la validation, la robustesse et la maîtrise des risques des modèles, essentielle pour répondre aux exigences prudentielles et de transparence.

Enfin, nos pôles sectoriels : Actuarial Services, Financial Markets & Investments, Sustainability accompagnent l'adaptation des modèles, systèmes d'information et obligations réglementaires dans les secteurs assurance, banque, gestion d'actifs et finance durable.

Notre cabinet offre une vision 2030 complète pour soutenir les institutions dans leur transformation : intégrer l'IA en toute confiance, anticiper les évolutions réglementaires et moderniser durablement leurs dispositifs de contrôle interne.

GLOSSAIRE

Finance Innovation

NEXIALOG CONSULTING

ACPR : Autorité de Contrôle Prudentiel et de Résolution

AI (IA) Act : Artificial Intelligence Act (Règlement européen sur l'intelligence artificielle – Règlement (UE) 2024/1689)

AI : Artificial Intelligence

AML : Anti-Money Laundering

AML/CFT : Anti-Money Laundering / Countering the Financing of Terrorism

API : Application Programming Interface

BCE : Banque Centrale Européenne

BCBS : Basel Committee on Banking Supervision

BCBS 239 : Principles for effective risk data aggregation and risk reporting

BIS : Bank for International Settlements

CA : Chiffre d'Affaires

CLM : Contract Lifecycle Management

CRM : Customer Relationship Management

DORA : Digital Operational Resilience Act

DPIA : Data Protection Impact Assessment

DSI : Direction des Systèmes d'Information

DQI : Data Quality Index

EAD : Exposure at Default

EBA : European Banking Authority

ECB : European Central Bank

EIOPA : European Insurance and Occupational Pensions Authority

ESB : Enterprise Service Bus

ESG : Environmental, Social and Governance

ESMA : European Securities and Markets Authority

ETL : Extract, Transform, Load

EU / UE : European Union / Union européenne

FRIA : Fundamental Rights Impact Assessment

RGPD : General Data Protection Regulation

GPAI : General Purpose Artificial Intelligence

GPU : Graphics Processing Unit

GRC : Governance, Risk and Compliance

HSBC : Hongkong and Shanghai Banking Corporation

IA : Intelligence Artificielle

IDD : Insurance Distribution Directive

IFRS 9 : International Financial Reporting Standard 9

ISO : International Organization for Standardization

IT : Information Technology

KPI : Key Performance Indicator

KRI : Key Risk Indicator

KYC : Know Your Customer

LCB-FT : Lutte contre le blanchiment de capitaux et le financement du terrorisme

LGD : Loss Given Default

LLM : Large Language Model

LoD / LOD : Line of Defense

MiFID II : Markets in Financial Instruments Directive II

MiFIR : Markets in Financial Instruments Regulation

ML : Machine Learning

MVP : Minimum Viable Product

NIS2 : Network and Information Security Directive 2

NLP : Natural Language Processing

OCDE : Organisation de Coopération et de Développement Économiques

PD : Probability of Default

POC : Proof of Concept

RACI : Responsible, Accountable, Consulted, Informed

RGPD : Règlement Général sur la Protection des Données

ROI : Return on Investment

RPA : Robotic Process Automation

RSSI : Responsable de la Sécurité des Systèmes d'Information

SHAP : SHapley Additive exPlanations

SIEM : Security Information and Event Management

SOX : Sarbanes-Oxley Act

SSM : Single Supervisory Mechanism

TIC : Technologies de l'Information et de la Communication

XAI : Explainable Artificial Intelligence

BIBLIOGRAPHIE

Finance Innovation

NEXIALOG CONSULTING

1. TEXTES RÉGLEMENTAIRES ET CADRES JURIDIQUES EUROPÉENS

- Union européenne (2024). Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act). Journal officiel de l'Union européenne, 12 juillet 2024. EUR-Lex.
- ACPR. Le règlement européen sur l'intelligence artificielle (AI Act). *https://acpr.banque-france.fr/fr/actualites/le-reglement-europeen-sur-lintelligence-artificielle-ai-act*
- ACPR. Règlement européen sur l'intelligence artificielle : comment l'ACPR se prépare-t-elle ? *https://acpr.banque-france.fr/fr/actualites/reglement-europeen-sur-lintelligence-artificielle-comment-lacpr-se-prepare-t-elle*
- Parlement européen et Conseil de l'Union européenne (2016). Règlement (UE) 2016/679 – Règlement général sur la protection des données (RGPD).
- European Data Protection Board (EDPB). Guidelines on Automated individual decision-making and Profiling (Article 22 GDPR).
- Union européenne (2022). Digital Operational Resilience Act (DORA).
- Union européenne (2022). Directive (UE) 2022/2555 – Network and Information Security Directive (NIS2).

2. DOCTRINE DES SUPERVISEURS FINANCIERS

BANQUE CENTRALE EUROPÉENNE / SUPERVISION BANCAIRE

- European Central Bank (ECB) (2024). From data to decisions: AI and supervision. *https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html*
- European Central Bank (ECB) (2024). Artificial intelligence: a central bank's view. *https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240704_1~e348c05894.en.html*
- European Central Bank (ECB) (2024). The rise of artificial intelligence: benefits and risks for financial stability. *https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html*
- European Central Bank (ECB) (2019). Bringing artificial intelligence to banking supervision.

AUTORITÉ BANCAIRE EUROPÉENNE (EBA)

- European Banking Authority (EBA) (2023). Follow-up Report on the use of machine learning for internal ratings-based models. *https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-follow-report-use-machine-learning-internal*
- European Banking Authority (EBA). Special Topic – Artificial Intelligence. *https://www.eba.europa.eu/publications-and-media/publications/special-topic-artificial-intelligence*
- European Banking Authority (EBA). Guidelines on Loan Origination and Monitoring ; Remote Customer Onboarding ; ML/TF Risk Factors ; Outsourcing Arrangements.

AUTORITÉS FRANÇAISES ET MARCHÉS FINANCIERS

- ACPR (2018). Intelligence artificielle : enjeux pour le secteur financier. *https://acpr.banque-france.fr/fr/publications-et-statistiques/publications/intelligence-artificielle-enjeux-pour-le-secteur-financier*
- ACPR (2020). Gouvernance des algorithmes d'intelligence artificielle dans le secteur financier. *https://acpr.banque-france.fr/fr/publications-et-statistiques/publications/gouvernance-des-algorithmes-dintelligence-artificielle-dans-le-secteur-financier*
- Autorité des Marchés Financiers (AMF) (2012). Organisation et missions de la fonction Conformité et Contrôle Interne (RCSI–RCCI), DOC-2012-17.
- European Securities and Markets Authority (ESMA) (2024). Artificial Intelligence and Investment Services – MiFID II expectations.

3. CADRES INTERNATIONAUX DE GOUVERNANCE ET GESTION DES RISQUES IA

- Organisation de Coopération et de Développement Économiques (OCDE). Principles on Artificial Intelligence. *https://www.oecd.org/en/topics/ai-principles.html*
- OCDE. Governing with Artificial Intelligence. *https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html*
- OCDE (2024). Regulatory approaches to Artificial Intelligence in finance.
- Bank for International Settlements (BIS) – Financial Stability Institute (2024). Regulating AI in the financial sector: recent developments and main challenges, FSI Insights No. 63. *https://www.bis.org/fsi/publ/insights63.pdf*
- National Institute of Standards and Technology (NIST) (2023). AI Risk Management Framework 1.0. *https://www.nist.gov/itl/ai-risk-management-framework*
- ISO/IEC (2023). ISO/IEC 42001 – Artificial Intelligence Management System. *https://www.iso.org/standard/81230.html*

4. ÉTUDES SECTORIELLES – BANQUE, ASSURANCE, CONFORMITÉ ET AUDIT

- Fédération Bancaire Française (FBF) (2025). Banques et intelligence artificielle générative : étude interbranches sur les métiers et compétences. *https://www.fbf.fr/fr/communique_de_presse/banques-et-intelligence-artificielle-une-etude-interbranches-sur-leurs-metiers-et-competences/*
- European Banking Federation (EBF). Position Paper on Artificial Intelligence. *https://www.ebf.eu/priorities/innovation-cybersecurity/artificial-intelligence/*
- Hub France IA. Contrôle des risques des systèmes d'intelligence artificielle (Livre blanc – BNP Paribas, La Banque Postale, Société Générale).
- Deloitte France. L'intelligence artificielle, un allié du contrôle interne ?
- Seabird. Conformité et contrôle interne : que peut apporter l'intelligence artificielle ?

5. CAS D'USAGE, REGTECH ET SOLUTIONS MARCHÉ

- CUBE (2025). CUBE acquires Acin to launch integrated risk and compliance solution.
- Sources : PR Newswire ; Fintech Futures ; IBS Intelligence ; A-Team Insight.
- Microsoft. RegBrain / CUBE – Regulatory mapping and AI-driven compliance (blog et publications officielles).
- Corlytics, Kodex AI, Cube – solutions de veille réglementaire et mapping automatisé.
- Actimize (NICE), Feedzai, SAS AML, Moody's Analytics, FICO, Shift Technology, Harmoney, CaseWare IDEA, KPMG Clara.

6. PROSPECTIVE, RISQUES ET IMPACTS MACROÉCONOMIQUES

- World Economic Forum (2024). AI in Financial Services Industry Survey. *www.weforum.org*
- World Economic Forum & Accenture (2025). Global Economic Futures: Productivity in 2030.
- World Economic Forum (2023). The Future of Jobs Report. *https://www.weforum.org/reports/the-future-of-jobs-report-2023/*
- Gartner (2025). Finance 2030: The Future of Finance.
- Gartner (2025). Eight Forces That Will Reshape the Finance Function Through 2030.
- Gartner Research (2024). AI bias in enterprise systems.
- Maple, C. et al. (2023). The AI Revolution: Opportunities and Challenges for the Finance Sector. arXiv. *https://arxiv.org/abs/2308.16538*

NEXIALOG
CONSULTING

Finance
Innovation