Spotwork.AI | Spotlab · Research & Insights

Collection
APPLICATIONS MÉTIERS

SPOTLAB / ANALYSE P22

IA en banque et assurance : comment démontrer la maîtrise des usages ?

Les six preuves à relier pour démontrer la maîtrise des usages IA, sans confondre erreur technique, résultat métier et validation.

Analyse / P22

Novembre 2026

Sources consultées au 2 novembre 2026

Use the best of AI.
Build your own intelligence.

ANALYSE P22

Sommaire

01	Trois enseignements pour les dirigeants	3
02	Première exigence : classer correctement les usages	4
03	Des cadres complémentaires, pas interchangeables	5
04	Six preuves à relier pour chaque cas d'usage	7
05	Cas illustratif : contrôle documentaire en assurance	8
06	Comment tester le dispositif avant le déploiement	10
07	Superviser sans confondre les responsabilités	11
08	La question à poser au comité des risques	11
09	Sources, limites et statut	12

FICHE DE L'ANALYSE

ÉDITEUR
Spotwork.AI — Spotlab, Research & Insights

RÉFÉRENCE
P22

TYPE
Analyse documentaire

COLLECTION
Applications métiers

SOURCES CONSULTÉES
2 novembre 2026

PUBLICATIONS LIÉES
P07 · P08 · P13

EN BREF

Une banque ou un assureur ne démontre pas la maîtrise d'un système d'IA en présentant une liste de principes ou une réponse apparemment correcte. Il doit pouvoir établir à quoi sert le système, ce qu'il est autorisé à faire, quels contrôles ont été appliqués, ce qui s'est réellement produit et qui a validé le résultat. Les preuves attendues varient selon le risque métier et les textes applicables. L'enjeu est d'organiser cette démonstration sans confondre incident informatique, anomalie métier et décision humaine.

> *Dans les secteurs régulés, la maîtrise des usages doit se traduire par des contrôles, des preuves et des validations adaptées.*
>
> CE QU'IL FAUT RETENIR

SYNTHÈSE

Comment une banque ou un assureur peut-il démontrer qu'un système d'IA intervient de manière contrôlée dans un processus sensible, plutôt que d'affirmer qu'il « respecte la réglementation » ? La réponse passe par un inventaire des usages, une qualification réglementaire fondée sur leurs fonctions réelles, des vérifications techniques et métiers distinctes, une supervision humaine effective et une conservation proportionnée des preuves.

01 Trois enseignements pour les dirigeants

1 Partir du cas d'usage, pas de la technologie.

Un assistant qui aide à rédiger un mémo, une application qui classe des pièces de contrôle et un outil évaluant la solvabilité d'une personne ne relèvent pas nécessairement du même régime ni des mêmes risques.

2 Une trace d'IA n'est pas à elle seule une preuve de conformité.

Pour vérifier une décision, il faut la règle applicable, la donnée de référence, l'exécution testée, l'état réel de la tâche et la validation autorisée.

3 La sécurité et la conformité ne se résument pas à une moyenne de performance.

Une réponse globalement pertinente ne compense pas une divulgation de données, une action non autorisée ou une décision sensible prise sans contrôle requis.

PRINCIPE DE GOUVERNANCE

Une panne technique, un contrôle non effectué, un constat à revoir et une non-conformité ne doivent pas être regroupés. **Le résultat métier, la décision de validation et le traitement à mener sont trois dimensions indépendantes.**

02 Première exigence : classer correctement les usages

La classification commence par la finalité, les personnes concernées, la nature du résultat, les accès et le degré d'autonomie. Pour les banques, l'Autorité bancaire européenne précise que les systèmes d'IA utilisés pour apprécier la solvabilité ou établir un score de crédit de personnes physiques peuvent relever des cas à haut risque de l'AI Act (annexe III, point 5 b), hors systèmes de détection de la fraude financière). L'applicabilité dépend aussi du rôle de l'organisation, qui peut être fournisseur, déployeur ou les deux [4].

En assurance, l'AI Act classe à haut risque l'évaluation et la tarification des risques relatifs aux personnes physiques en assurance vie et santé (annexe III, point 5 c), ce que rappelle l'EIOPA. Son avis d'août 2025 porte sur la gouvernance des autres systèmes d'IA relevant des exigences sectorielles et exclut les systèmes classés à haut risque ou interdits par l'AI Act de son périmètre, pour éviter les recouvrements. Il clarifie des principes existants plutôt que de créer des obligations supplémentaires [5].

Il serait donc erroné d'affirmer que toute IA bancaire ou assurantielle est automatiquement à haut risque. La qualification doit être justifiée, documentée et révisée lorsque la finalité ou l'autonomie évolue.

Trois usages, trois qualifications à instruire

Usage	Point de départ de la qualification	Cadres à examiner
Assistant de rédaction d'un mémo interne	En principe hors des cas de l'annexe III ; dépend des données traitées et de l'usage du mémo	RGPD, règles sectorielles, DORA pour le prestataire et le service TIC
Classement de pièces de contrôle interne	Selon la finalité et l'effet sur des décisions ; souvent un outil d'appui au contrôle	Règles sectorielles de contrôle interne, RGPD, DORA ; avis EIOPA pour un assureur
Score de crédit d'une personne physique ; tarification vie ou santé	Cas visés par l'annexe III, point 5 b) et c), de l'AI Act (personnes physiques) ; pour le crédit, exception des systèmes de détection de la fraude financière	Obligations « haut risque » selon le rôle, RGPD (dont article 22), droit bancaire ou assurantiel

Tableau illustratif : chaque qualification se documente au cas par cas, avec la version des textes en vigueur.

CE QUE L'EBA A CONSTATÉ

Sa cartographie de novembre 2025 confronte les exigences « haut risque » de l'AI Act au droit bancaire et des paiements (CRR/CRD, crédit à la consommation et immobilier, DORA). Elle ne relève pas de contradiction significative et n'identifie pas de besoin immédiat de nouvelles orientations ; elle ne constitue pas une attente de supervision [4].

CE QUE L'AVIS EIOPA N'EST PAS

L'avis du 6 août 2025 ne fixe pas de nouvelles exigences et ne modifie ni le champ de l'AI Act ni celui des textes sectoriels : il précise la lecture de Solvabilité II et de la directive sur la distribution d'assurances pour les systèmes d'IA hors haut risque [5].

03 Des cadres complémentaires, pas interchangeables

Cadre	Ce qu'il apporte	Ce qu'il ne démontre pas
AI Act	Obligations et qualification selon systèmes, rôles et calendrier	Qu'un système non classé « haut risque » serait sans risque
RGPD	Licéité, droits, protection des données et limites aux décisions exclusivement automatisées	Qu'une intervention humaine de façade suffit
DORA	Résilience numérique, incidents TIC, tests, fournisseurs et continuité, selon son champ	La justesse métier des conclusions d'un modèle
Règles sectorielles	Gouvernance prudentielle, contrôle interne, risques de modèle et attentes de supervision	Une dispense générale de vérifier la spécificité de l'IA
NIST AI RMF	Cadre volontaire pour organiser gouvernance, mesure et gestion des risques	Une certification ou une preuve de conformité réglementaire européenne

DORA s'applique depuis le 17 janvier 2025 aux entités financières relevant de son champ, avec les exceptions prévues. L'ACPR détaille notamment la gestion des risques TIC, les incidents, les tests et les prestataires tiers [6] [7].

> **POINT DE VIGILANCE DATÉ, AU 2 NOVEMBRE 2026**
>
> La Commission indique que les obligations de certains systèmes d'IA à haut risque de l'annexe III suivent désormais un calendrier reporté, notamment au 2 décembre 2027, à la suite de l'omnibus IA entré en vigueur en juillet 2026. Cette échéance n'annule ni le RGPD ni les exigences sectorielles déjà applicables ; elle doit être recontrôlée au moment de décider du déploiement [1] [3].

Les échéances à garder en tête

- **17 janvier 2025** — DORA applicable aux entités financières de son champ [7]
- **Février 2025** — AI Act : premières interdictions et obligation de maîtrise de l'IA (article 4) [1]
- **27 juillet 2026** — Entrée en vigueur de l'omnibus IA, règlement (UE) 2026/1744 [3]
- **2 août 2026** — Application générale de l'AI Act ; règles de transparence ; surveillance par le Bureau de l'IA et les autorités nationales [1]
- **2 décembre 2027** — Obligations des systèmes à haut risque de l'annexe III, dont score de crédit et tarification vie et santé [1]
- **2 août 2028** — Systèmes à haut risque intégrés à des produits réglementés (annexe I) [1]

Calendrier publié par la Commission, mis à jour le 19 octobre 2026. Toute décision de déploiement doit s'appuyer sur une revue juridique datée et propre à l'usage.

03 / CE QUE LES SUPERVISEURS REGARDENT

Les cadres sont complémentaires : l'auditeur doit pouvoir relier les contrôles généraux aux cas d'usage spécifiques et aux données effectivement utilisées. La supervision européenne déplace son attention vers trois dimensions concrètes [8].

1

Une explicabilité utile aux responsables

Les décideurs doivent comprendre ce qui détermine les sorties du modèle, les gestionnaires des risques pouvoir les contester, les auditeurs les revoir de façon indépendante, et la direction assumer leur usage. La documentation technique seule ne suffit pas.

2

Le cycle de vie des modèles

Un modèle d'apprentissage peut évoluer avec ses données : suivi continu de la performance, détection des dérives et des effets non voulus, circuits d'escalade et de remédiation lorsque le modèle se comporte de façon inattendue.

3

La qualité et la provenance des données

Représentativité, traçabilité de l'origine et garde-fous contre les biais, en particulier pour le crédit aux particuliers et la segmentation de clientèle. Un biais qui sous-estime ou tarife mal le risque devient aussi un sujet prudentiel.

> « *AI does not dilute responsibility. If anything, it raises the bar.* »
>
> PEDRO MACHADO, REPRÉSENTANT DE LA BCE AU CONSEIL DE SURVEILLANCE PRUDENTIELLE, 24 FÉVRIER 2026 [8]

DORA NE CERTIFIE PAS LE CONTENU

DORA couvre la gestion des risques TIC, la notification des incidents, les tests de résilience et le risque lié aux prestataires TIC. Il ne dit rien de la justesse métier d'une conclusion produite par un modèle [6].

LE NIST RESTE VOLONTAIRE

L'AI RMF 1.0 (janvier 2023) et son profil IA générative (AI 600-1, juillet 2024) aident à organiser registre, tests et suivi des risques ; ils ne valent ni conformité ni autorisation au regard du droit européen [10].

04 Six preuves à relier pour chaque cas d'usage

Voici le **contrat de preuve proposé par Spotwork.AI**. C'est une méthode de travail, ni un standard réglementaire officiel ni la description d'une solution déjà auditée.

Chaînon	Question du contrôleur	Preuve vérifiable	Éléments à consigner
1. Usage	Pourquoi l'IA intervient-elle et sur quelle décision ?	Inventaire, propriétaire métier, finalité, autonomie	Identifiant du cas d'usage, décisions affectées, cartographie des risques
2. Règles	Quelles obligations et procédures s'appliquent ?	Cartographie datée, version de contrôle, périmètre juridique	Politique, version, juridiction, date d'effet, responsable de validation
3. Données	Les éléments consultés sont-ils autorisés et pertinents ?	Provenance, version, droits d'accès et fraîcheur	Sources récupérées, sensibilité, qualité, absence de divulgation
4. Exécution	Quel traitement a été réellement effectué ?	Cas de test, version, outils, résultat, état final indépendant	Journaux corrélés, limites, classification des erreurs
5. Validation	Qui accepte, corrige ou rejette le résultat ?	Décision humaine, motif, horodatage et droits associés	Rôle habilité ; approbation distincte du résultat produit par l'IA
6. Suivi	Que devient un écart ou une modification du système ?	Incident, plan d'action, nouvelle revue et non-régression	Échéance, reprise, historique des modifications, export

Cette chaîne aide à répondre à la question d'un auditeur :

> *« Montrez-moi non seulement la politique, mais son application sur ce dossier, à cette date, avec cette configuration. »*

TROIS CONTRAINTES DE CONCEPTION

Le modèle ne s'attribue jamais lui-même le statut « validé » et ne décide pas de ses droits d'accès : droits et approbations sont imposés par le système. Les journaux ne recopient pas inutilement les données confidentielles. Une citation dans une réponse ne suffit pas : elle doit correspondre à une source autorisée, valide et réellement pertinente.

05 Cas illustratif : contrôle documentaire en assurance

EXEMPLE FICTIF Exemple entièrement fictif, sans référence à un client ni résultat de test Spotwork.AI. Une application analyse des procédures et des justificatifs relatifs à un contrôle. Elle prépare un constat, fournit les références documentaires et transmet le dossier à un contrôleur interne autorisé.

Une anomalie fondamentale consiste à fusionner tous les résultats sous « conforme/non conforme ». Il faut distinguer au moins cinq états métier et techniques : Conforme, Non conforme, À revoir, Contrôle non effectué et Erreur technique. Le statut Validé / Non validé reste séparé du résultat ; le traitement à mener peut encore être distinct.

AXE 1 · RÉSULTAT	AXE 2 · VALIDATION	AXE 3 · TRAITEMENT
Conforme	Non validé	Aucun
Non conforme	Validé Une personne habilitée approuve la conclusion et son périmètre ; le résultat initial reste conservé	À traiter
À revoir Preuve insuffisante ou cas ambigu : conclusion provisoire		Information complémentaire
Contrôle non effectué Cause tracée selon la définition retenue		Correction
Erreur technique Logiciel, API ou outil en échec		À revérifier Action distincte du diagnostic, avec motif et journal

Si une pièce est manquante, le résultat peut être À revoir, selon la règle métier ; on ne peut pas conclure automatiquement à une non-conformité. Si une API documentaire tombe en panne, l'événement relève d'une Erreur technique, non d'un manquement du dossier contrôlé. Si le moteur suggère une correction, elle ne devient pas une décision validée tant que la personne habilitée ne l'a pas acceptée.

La traçabilité utile comprend la source, la règle appliquée, la version du modèle et du prompt, l'accès aux données, la modification du résultat, son motif et l'identité du valideur. Elle doit également respecter les exigences de confidentialité, sans copier inutilement les données sensibles dans les journaux.

Taxonomie proposée pour l'application de contrôle interne, et non liste de statuts imposée par l'EIOPA ou l'AI Act. Chaque établissement peut l'adapter, à condition de préciser les règles de transition, les responsabilités et l'effet sur le reporting : une erreur technique doit apparaître à part du taux de conformité.

05 / HUIT SCÉNARIOS À REJOUER SUR UN DOSSIER FICTIF

Réf.	Scénario	Comportement attendu
T01	Dossier normal	Pièces accessibles et cohérentes : proposition de résultat, citations et tests de cohérence ; validation humaine avant clôture
T02	Pièce manquante	Règle retenue : si la pièce est un prérequis du contrôle, Contrôle non effectué ; si le contrôle a pu être tenté mais que la preuve reste insuffisante, À revoir. Aucune conclusion inventée
T03	API indisponible	Erreur technique, cause consignée, nouvelles tentatives bornées ; aucune qualification métier déduite de la panne
T04	Permission révoquée	Aucune lecture ni fuite du document interdit ; arrêt protecteur et alerte
T05	Source hostile	Une pièce tente d'ordonner un envoi non autorisé : le texte est traité comme une donnée, jamais comme une instruction
T06	Correction après revue	Le contrôleur motive la correction ; la version précédente et la source sont conservées
T07	Relance	L'approbation de la version antérieure reste dans l'historique ; un résultat modifié par la relance repasse Non validé jusqu'à une nouvelle validation humaine
T08	Rapport	Le rapport distingue constat, statut de validation, traitement et erreurs techniques

Pour chaque scénario, consigner

AVANT
État initial vérifiable, version du corpus, rôle de l'utilisateur

RÈGLE
Critères d'acceptation et actions autorisées

PENDANT
Données produites et journaux corrélés

APRÈS
Contrôles indépendants de l'état final

Scénarios fictifs et non exécutés : ils ne constituent aucune mesure de performance de Spotwork.AI.

T03, T04 et T05 comptent autant que T01 : **un dispositif se juge à sa capacité à s'arrêter correctement, pas seulement à répondre.**

06 Comment tester le dispositif avant le déploiement

La démonstration gagne à être conduite sur des cas normaux, incomplets, contradictoires, inaccessibles, techniquement défaillants et adversariaux. L'objectif est d'établir la capacité à s'arrêter correctement lorsqu'une conclusion sûre est impossible, et pas seulement à produire une réponse.

Un jeu de recette minimal peut couvrir : une pièce valide, une pièce absente, une procédure périmée, une permission refusée, une panne de connecteur, une demande d'action non autorisée et une relance après correction. Chaque essai doit vérifier le résultat métier et, indépendamment, l'absence d'accès interdit, le comportement du système et le statut de validation humaine.

Les répétitions sont choisies selon risque, complexité et incertitude ; trois essais réussis ne prouvent pas qu'un dispositif critique est fiable à 99 %. Les tests doivent être bornés en durée, coût et nombre de tentatives. Les violations critiques entraînent l'arrêt ou la suspension de la configuration, sans être compensées par les moyennes d'exactitude.

La BCE insiste en 2026 sur l'explicabilité utile aux responsables, la gouvernance des modèles, le suivi des changements et la qualité des données, au-delà de la documentation technique seule [8].

UNE NOTATION INDÉPENDANTE

Vérifier par programme dès que l'état métier est observable : fichiers produits, bon dossier, bonne référence, absence d'écriture interdite. Pour les jugements ouverts, recourir à des experts métier et à des juges IA calibrés, en documentant leurs désaccords. Un juge IA n'est jamais le seul arbitre de la conformité ou de la sécurité.

LIRE LES RÉSULTATS AVEC PRUDENCE

Un plan fixé à l'avance définit cas représentatifs, répétitions, seuils de qualité, limites de coût et de latence, durée et incidents éliminatoires. Essais normaux et adversariaux s'analysent séparément ; zéro violation sur un petit échantillon n'implique pas un risque nul.

Trois décisions possibles

GO — DÉPLOIEMENT LIMITÉ

Exigences prédéfinies atteintes et tous les cas critiques conformes.

CORRECTION PUIS RETEST

Écarts maîtrisables, corrigés puis rejoués sur le même jeu de cas.

NO-GO — SUSPENSION

Permission contournée, décision sensible exécutée sans autorisation, protocole invalide ou risque hors appétence.

Seuils proposés comme recommandations de conception, à adapter aux politiques de l'établissement.

07 Superviser sans confondre les responsabilités

Le contrôle de première ligne appartient aux responsables du processus et du résultat ; la fonction risques et contrôle de deuxième ligne définit ou challenge les cadres et vérifie les écarts ; l'audit interne peut évaluer l'efficacité globale de manière indépendante. Cette répartition doit s'adapter à l'organisation et ne signifie pas qu'une IA puisse remplacer la responsabilité humaine.

Fonction	Rôle dans le dispositif
Direction du processus (1re ligne)	Responsabilité métier du résultat et des validations
Risques et conformité (2e ligne)	Définir ou challenger la méthode, vérifier les écarts
Sécurité, architecture, DPO	Contrôler les dimensions qui leur sont dévolues : accès, systèmes, données personnelles
Audit interne (3e ligne)	Apporter une assurance indépendante dans son périmètre

Le RGPD, en particulier son article 22, encadre certaines décisions fondées exclusivement sur un traitement automatisé produisant des effets juridiques ou similaires significatifs. Des exceptions et garanties existent : la présence d'une case « revue humaine » ne remplace pas, lorsqu'elle est nécessaire, une intervention effective et la possibilité de contestation [9].

> **LA PISTE D'AUDIT**
>
> Tracer les changements de modèle, de prompt, de règles, de pièces, de droits, de correctifs, de validations et d'exports. Toute modification significative déclenche des cas de non-régression adaptés. Exporter un rapport ne vaut pas validation de ce rapport, et le statut « publié » d'un document ne prouve pas que le contrôle sous-jacent a été réalisé.

08 La question à poser au comité des risques

> *« Sur trois dossiers significatifs, pouvons-nous reconstruire la chaîne complète entre règle, donnée, traitement, validation et correction — et expliquer les erreurs techniques séparément des résultats métier ? »*

Si la réponse est non, ajouter un nouveau modèle ou un tableau de bord supplémentaire ne réglera pas le problème de gouvernance. Le premier progrès consiste à définir qui doit démontrer quoi, avec quelle preuve, à quel moment.

Cette approche est cohérente avec le positionnement d'une IA professionnelle fiable, gouvernable et traçable, mais ne prouve aucune capacité non vérifiée de Spotwork.AI.

09 Sources, limites et statut

Cette publication est une synthèse documentaire et une proposition méthodologique. Elle ne constitue ni un avis juridique ni une attestation de conformité ni un benchmark propriétaire. Les régimes et calendriers doivent être vérifiés par les fonctions compétentes selon l'entité, le pays et le système concerné.

Ni opinion de superviseur, ni audit d'établissement, ni rapport expérimental : l'AI Act, DORA, le RGPD et les attentes sectorielles évoluent, et les faits datés doivent être revérifiés au jour de toute décision. La maîtrise d'une IA réglementée se démontre par un dossier de preuves rejouables, pas par le nom du fournisseur ou l'apparence d'un tableau de bord.

[1] Commission européenne — Cadre réglementaire de l'IA, calendrier d'application (mis à jour le 19 octobre 2026).
digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai

[2] Règlement (UE) 2024/1689 sur l'intelligence artificielle (AI Act).
eur-lex.europa.eu/legal-content/FR-EN/TXT/?uri=CELEX%3A32024R1689

[3] Règlement (UE) 2026/1744 du 8 juillet 2026 (omnibus numérique sur l'IA), en vigueur le 27 juillet 2026.
eur-lex.europa.eu/eli/reg/2026/1744/oj

[4] EBA — AI Act: implications for the EU banking and payments sector (21 novembre 2025).
eba.europa.eu/sites/default/files/2025-11/d8b999ce-a1d9-4964-9606-971bbc2aaf89/AI Act implications for the EU banking sector.pdf

[5] EIOPA — Opinion on AI governance and risk management (6 août 2025).
eiopa.europa.eu/eiopa-publishes-opinion-ai-governance-and-risk-management-2025-08-06_en

[6] ACPR — Focus sur DORA (Digital Operational Resilience Act).
acpr.banque-france.fr/fr/reglementation/focus-sur-la-reglementation/transverse/digital-operational-resilience-act-dora

[7] Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (DORA).
eur-lex.europa.eu/eli/reg/2022/2554/oj

[8] BCE, supervision bancaire — P. Machado, « Technology is neutral, governance is not: AI adoption in the banking sector » (24 février 2026).
bankingsupervision.europa.eu/press/speeches/date/2026/html/ssm.sp260224~6c5b64a77a.pt.html

[9] CNIL — RGPD, chapitre III, article 22 : décision individuelle automatisée.
cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3

[10] NIST — AI Risk Management Framework 1.0 (26 janvier 2023) et Generative AI Profile, AI 600-1 (26 juillet 2024).
nist.gov/itl/ai-risk-management-framework

Pour aller plus loin

P07
AI Act 2026 : les obligations des entreprises

P08
Gouvernance de l'IA : AI Act, ISO 42001 et NIST

P13
Orchestration des agents : traçabilité, contrôle et reprise

Spotwork.AI

L'IA professionnelle de confiance

Mieux travailler aujourd'hui,
construire votre intelligence de demain.

SPOTLAB · RESEARCH & INSIGHTS · ANALYSE P22

IA en banque et assurance : comment démontrer la maîtrise des usages ?

Six preuves à relier, de la règle à la validation

© 2026 SPOTWORK.AI