

# L'adoption responsable de l'intelligence artificielle dans la finance

Lecture analytique des 12 pratiques saines du  
Conseil de stabilité financière (FSB, 2026)  
**et projection sur le système financier marocain**

12

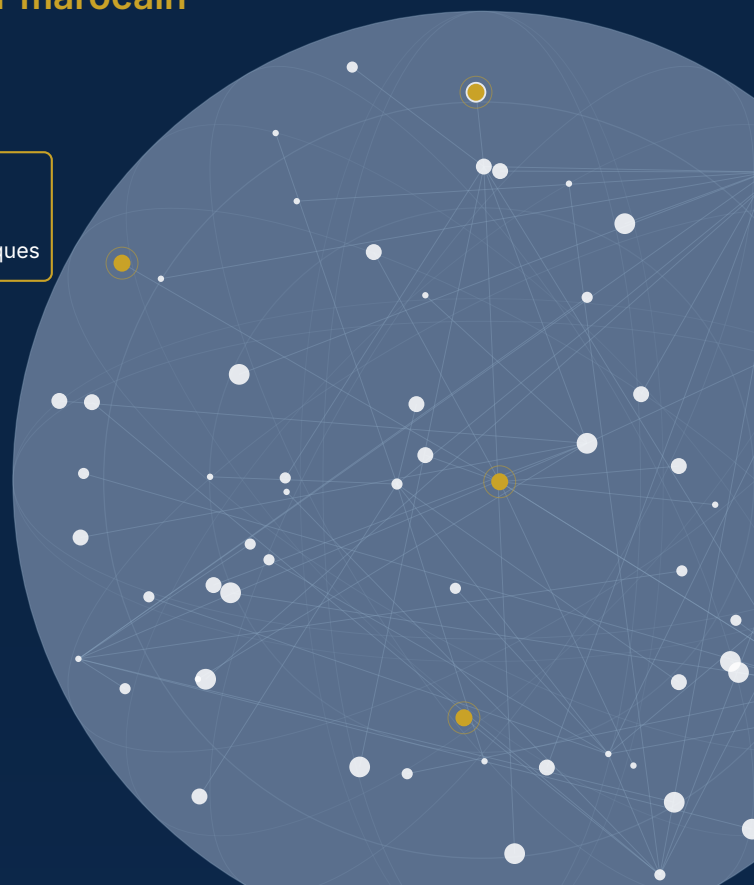
pratiques saines

7

étapes du  
cycle de vie

9

familles de risques



RÉALISÉ PAR

**Imad EL KHLIFI**

DOCUMENT DE RÉFÉRENCE

FSB, Sound Practices for Responsible  
Adoption of Artificial Intelligence  
Rapport final, 15 octobre 2026

# Avant-propos

Le 15 octobre 2026, le Conseil de stabilité financière (*Financial Stability Board*, FSB) a publié la version finale de son rapport *Sound Practices for Responsible Adoption of Artificial Intelligence (AI)*. Ce document clôt un processus engagé avec une consultation publique en juin 2026 et prolonge deux travaux antérieurs du FSB consacrés aux implications de l'intelligence artificielle (IA) pour la stabilité financière, publiés respectivement en 2017 et en 2024. Il propose douze pratiques saines destinées à aider les institutions financières à tirer parti de l'IA tout en maîtrisant les risques qu'elle crée ou amplifie.

La présente note poursuit trois objectifs complémentaires. Le premier est **restitutif** : présenter de manière ordonnée, en langue française, l'essentiel du contenu du rapport, qu'il s'agisse de l'état de l'adoption de l'IA, de la cartographie des risques ou des douze pratiques elles-mêmes. Le deuxième est **analytique** : dégager la logique d'ensemble du dispositif proposé, ses apports par rapport aux cadres existants et ses zones d'incertitude, notamment en matière d'IA agentique. Le troisième est **prospectif** : interroger la portée de ces recommandations pour le système financier marocain, au regard de son architecture de supervision, de son cadre juridique en matière de données et de cybersécurité, et de son niveau de maturité numérique.

## Note de méthode

Les données chiffrées citées dans les chapitres 1 à 4 proviennent exclusivement du rapport du FSB et des études de cas qu'il rapporte. Ces études ont, selon le FSB lui-même, une valeur illustrative : elles ne constituent ni des normes ni des résultats attendus. Les graphiques construits à partir de ces chiffres en reprennent fidèlement les valeurs. Les schémas conceptuels (matrice matérialité-risque, arbitrage explicabilité-performance) traduisent visuellement le raisonnement du rapport sans prétendre à une mesure empirique. Enfin, la grille de maturité présentée au chapitre 5 relève d'une appréciation qualitative de l'auteur et doit être lue comme une proposition de discussion, non comme une évaluation officielle.

Le document s'organise en six chapitres. Après une synthèse exécutive, le chapitre 1 dresse le panorama des usages de l'IA dans les différents segments du secteur financier. Le chapitre 2 présente la typologie des risques et des difficultés de mise en œuvre. Les chapitres 3 et 4 détaillent respectivement les quatre pratiques relatives à la gouvernance de l'organisation et les huit pratiques relatives à la gestion du cycle de vie de l'IA. Le chapitre 5 est consacré à la projection sur le Maroc et propose une feuille de route. Le chapitre 6 conclut. Des annexes rassemblent la liste des douze pratiques, un glossaire bilingue et les références.

# Table des matières

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>Avant-propos</b>                                                     | <b>ii</b> |
| <b>Synthèse exécutive</b>                                               | <b>2</b>  |
| <b>1 Le rapport et le paysage de l'adoption de l'IA dans la finance</b> | <b>4</b>  |
| 1.1 Genèse, statut et portée du rapport . . . . .                       | 4         |
| 1.2 Les moteurs de l'adoption . . . . .                                 | 5         |
| 1.3 Une adoption différenciée selon les segments . . . . .              | 5         |
| 1.4 Les cas d'usage et les bénéfices rapportés . . . . .                | 6         |
| <b>2 Cartographie des risques et des difficultés de mise en œuvre</b>   | <b>9</b>  |
| 2.1 Des vulnérabilités systémiques aux risques opérationnels . . . . .  | 9         |
| 2.2 Gouvernance inadéquate et défaut d'exécution stratégique . . . . .  | 9         |
| 2.3 Gouvernance et qualité des données défailtantes . . . . .           | 10        |
| 2.4 Les défis de l'explicabilité . . . . .                              | 10        |
| 2.5 Performance insuffisante ou dégradée. . . . .                       | 10        |
| 2.6 Supervision humaine inadaptée . . . . .                             | 10        |
| 2.7 Risques cyber et TIC . . . . .                                      | 10        |
| 2.8 Dépendances envers les tiers et concentration . . . . .             | 10        |
| 2.9 Protection des consommateurs et conduite de marché. . . . .         | 11        |
| 2.10 Les risques propres à l'IA agentique . . . . .                     | 12        |
| <b>3 La gouvernance de l'IA à l'échelle de l'organisation</b>           | <b>13</b> |
| 3.1 Orientation stratégique et supervision . . . . .                    | 13        |
| 3.2 Gouvernance et responsabilité . . . . .                             | 14        |
| 3.3 Cadre de gestion des risques et documentation . . . . .             | 14        |
| 3.4 Adaptabilité organisationnelle . . . . .                            | 15        |
| <b>4 La gestion des risques tout au long du cycle de vie de l'IA</b>    | <b>17</b> |
| 4.1 Un cycle de vie en sept étapes . . . . .                            | 17        |
| 4.2 Évaluation de la matérialité et du risque . . . . .                 | 17        |
| 4.3 Processus de sélection. . . . .                                     | 18        |
| 4.4 Gouvernance des données . . . . .                                   | 19        |
| 4.5 Explicabilité et transparence . . . . .                             | 19        |

|          |                                                                  |           |
|----------|------------------------------------------------------------------|-----------|
| 4.6      | Gestion de la performance . . . . .                              | 20        |
| 4.7      | Supervision humaine . . . . .                                    | 21        |
| 4.8      | Risques cyber et TIC . . . . .                                   | 22        |
| 4.9      | Risques liés aux tiers . . . . .                                 | 22        |
| <b>5</b> | <b>Projection sur le système financier marocain</b>              | <b>24</b> |
| 5.1      | Un socle institutionnel et juridique déjà structuré . . . . .    | 24        |
| 5.2      | Les spécificités qui conditionnent la transposition . . . . .    | 24        |
| 5.3      | Des opportunités alignées sur les priorités nationales . . . . . | 26        |
| 5.4      | Grille d'appréciation de la maturité . . . . .                   | 26        |
| 5.5      | Transposition des douze pratiques : propositions . . . . .       | 26        |
| 5.6      | Feuille de route en trois horizons . . . . .                     | 28        |
| <b>6</b> | <b>Conclusion : de la prudence à la maîtrise</b>                 | <b>29</b> |
|          | <b>Annexes</b>                                                   | <b>30</b> |

# Table des figures

|     |                                                                                                                   |    |
|-----|-------------------------------------------------------------------------------------------------------------------|----|
| 1   | Architecture des douze pratiques saines du FSB . . . . .                                                          | 3  |
| 1.1 | Jalons des travaux du FSB sur l'intelligence artificielle . . . . .                                               | 4  |
| 1.2 | Bénéfices rapportés dans les études de cas du FSB (valeurs «plus de» ou «environ») . . . . .                      | 7  |
| 1.3 | Compression des délais de traitement dans deux études de cas du FSB . . . . .                                     | 7  |
| 2.1 | Les quatre vulnérabilités systémiques et leurs amplificateurs récents . . . . .                                   | 9  |
| 2.2 | Les couches de la chaîne d'approvisionnement de l'IA . . . . .                                                    | 11 |
| 2.3 | Les sept familles de risques de l'IA agentique . . . . .                                                          | 12 |
| 3.1 | Les trois lignes de défense appliquées à l'IA . . . . .                                                           | 14 |
| 3.2 | La pyramide des compétences proposée par le FSB . . . . .                                                         | 15 |
| 4.1 | Le cycle de vie illustratif de l'IA selon le FSB . . . . .                                                        | 17 |
| 4.2 | Matrice matérialité-risque et proportionnalité des contrôles (schéma conceptuel) . . . . .                        | 18 |
| 4.3 | Les étapes de gestion des données destinées à l'IA . . . . .                                                      | 19 |
| 4.4 | L'arbitrage explicabilité-performance (schéma conceptuel) . . . . .                                               | 20 |
| 4.5 | Les formes de supervision humaine recensées par le FSB . . . . .                                                  | 21 |
| 5.1 | Les acteurs marocains concernés par l'adoption de l'IA dans la finance . . . . .                                  | 24 |
| 5.2 | Maturité du système financier marocain face aux pratiques du FSB (appréciation qualitative de l'auteur) . . . . . | 27 |
| 5.3 | Feuille de route proposée pour l'adoption responsable de l'IA au Maroc . . . . .                                  | 28 |

# Synthèse exécutive

**Un constat de départ : une adoption rapide, des risques en mutation.** Les institutions financières adoptent l'IA à un rythme soutenu pour gagner en efficacité, transformer leurs modèles d'affaires, améliorer le service à la clientèle et renforcer la gestion des risques. Le FSB observe que cette dynamique s'est accélérée depuis son rapport de 2024, avec des écarts importants selon les entités, les secteurs et les juridictions. À mesure que l'adoption gagne en ampleur et en sophistication, l'IA peut amplifier des risques existants et en faire naître de nouveaux : modèles peu explicables qui fragilisent la transparence, agents autonomes susceptibles d'agir hors des limites prévues, modèles avancés capables d'accroître la vitesse et l'ampleur des cyberattaques.

**Une idée directrice : l'adoption responsable.** Le rapport ne cherche ni à freiner ni à prescrire l'adoption. Il défend l'idée qu'une adoption responsable permet de saisir les opportunités tout en minimisant les risques, et qu'elle contribue, à l'échelle du système, à réduire les risques pour la stabilité financière. Il rappelle aussi, de manière notable, que *ne pas adopter* l'IA comporte des risques : perte de compétitivité et capacité amoindrie à détecter la fraude et les cybermenaces.

**12**

pratiques saines  
non contraignantes

**4**

pratiques de  
gouvernance de  
l'organisation

**8**

pratiques de gestion  
du cycle de vie

**Une architecture en deux blocs.** Les quatre premières pratiques portent sur la gouvernance de l'organisation : rôle central du conseil d'administration et de la direction générale (PS1), rôles et responsabilités clairement définis (PS2), intégration des risques de l'IA dans le cadre de gestion des risques et documentation effective (PS3), capacité d'apprentissage et d'adaptation (PS4). Les huit suivantes couvrent le cycle de vie de l'IA, de sa conception à son retrait : évaluation de la matérialité et du risque (PS5), sélection des technologies (PS6), gouvernance des données (PS7), explicabilité et transparence (PS8), gestion de la performance (PS9), supervision humaine (PS10), risques cyber et TIC (PS11) et risques liés aux tiers (PS12).

**Le principe de proportionnalité comme fil conducteur.** Les pratiques doivent être appliquées à proportion du modèle d'affaires, de la complexité, de la taille, du degré d'interconnexion et de l'usage de l'IA dans les fonctions critiques. Les établissements de petite taille et les cas d'usage peu matériels peuvent n'appliquer que les pratiques pertinentes, ou les adapter. Ce principe est décisif pour les systèmes financiers émergents, où coexistent de grands groupes bancaires panafricains et des acteurs plus modestes.

**Les apports de la version finale.** Par rapport au document de consultation de juin 2026, le rapport final reconnaît l'IA comme technologie d'augmentation et « multiplicateur de main-d'œuvre », tout en signalant le risque de déqualification des personnels. Il précise le rôle des conseils d'administration (y compris pour les petits établissements), enrichit les exigences de documentation, renforce la transparence pour les cas d'usage les plus matériels, élargit la gestion des risques liés aux tiers et ajoute des considérations spécifiques à l'IA agentique et aux systèmes multi-agents.

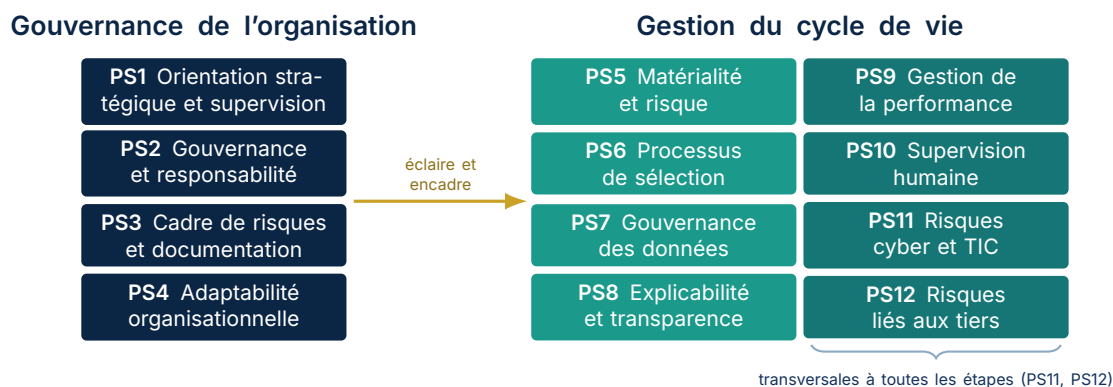


**FIG. 1** : Architecture des douze pratiques saines du FSB

### ★ Ce qu'il faut retenir pour le Maroc

Le Maroc dispose de briques solides pour accueillir ces pratiques : une supervision sectorielle structurée (Bank Al-Maghrib, AMMC, ACAPS), un cadre de protection des données personnelles (loi 09-08 et CNDP), une loi sur la cybersécurité (loi 05-20) et une stratégie numérique nationale (Maroc Digital 2030). Les principaux chantiers concernent l'absence, à ce jour, d'un référentiel prudentiel spécifique à l'IA, la gestion des dépendances envers des fournisseurs étrangers d'infrastructures et de modèles, la disponibilité de compétences spécialisées et l'adaptation des modèles de langage aux réalités linguistiques du pays (arabe, darija, amazighe, français). Le chapitre 5 propose une feuille de route en trois horizons.

# Le rapport et le paysage de l'adoption de l'IA dans la finance

## 1.1 Genèse, statut et portée du rapport

Le FSB coordonne, au niveau international, les travaux des autorités financières nationales et des organismes normalisateurs (*standard-setting bodies*, SSB) en vue de promouvoir des politiques de régulation et de supervision efficaces. Ses travaux, conformément à sa charte, ne créent ni obligation juridique ni droit. Le rapport de 2026 s'inscrit dans cette tradition : les douze pratiques sont **non prescriptives** et ne constituent pas une norme internationale contraignante. Elles se présentent comme une « boîte à outils » que chaque établissement adapte à son contexte et à son profil de risque, et qu'il peut intégrer dans ses cadres existants, notamment ceux relatifs au risque cyber et au risque lié aux tiers.

Le document s'appuie sur une trajectoire institutionnelle bien identifiée. En 2017, le FSB publiait une première analyse de l'IA et de l'apprentissage automatique dans les services financiers. En 2024, il actualisait son évaluation des implications de l'IA pour la stabilité financière en mettant en exergue quatre vulnérabilités : dépendances envers les tiers et concentration des prestataires, corrélations de marché, risques cyber, et enfin risque de modèle, qualité des données et gouvernance. En 2025, il publiait un rapport sur le suivi de l'adoption et des vulnérabilités. Le rapport de 2026 franchit une étape supplémentaire en passant du *diagnostic* à la *pratique*.

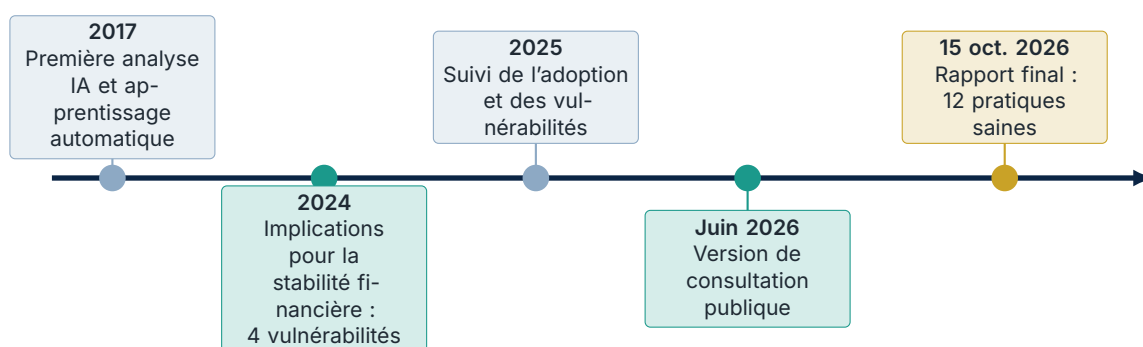


FIG. 1.1 : Jalons des travaux du FSB sur l'intelligence artificielle

Le rapport précise trois limites de son propre champ. D'abord, l'application des pratiques n'exonère pas l'établissement de ses obligations légales et réglementaires locales. Ensuite, les pratiques ne sont pas exhaustives et évolueront avec la technologie, en particulier pour l'IA agentique et les systèmes multi-agents, dont le traitement reste qualifié de « naissant ». Enfin, les études de cas sont illustratives et ne fixent aucun résultat de référence.

1.2 Les moteurs de l'adoption

Le FSB analyse l'adoption comme le produit de facteurs d'offre et de demande. Du côté de l'offre, les progrès de la puissance de calcul, notamment via l'informatique en nuage, la croissance des données disponibles et la diffusion des modèles de fondation ont abaissé les barrières à l'entrée. Du côté de la demande, les institutions cherchent à consolider leur position concurrentielle sur des marchés de plus en plus numériques, à améliorer leur efficacité opérationnelle et à renforcer leur gestion des risques.

1.2.1 Une diversification des familles technologiques

Le rapport distingue plusieurs générations d'IA, dont la coexistence au sein d'un même établissement complique la gouvernance.

| Famille                                        | Caractéristique principale                                                                                                                                                   | Enjeu dominant                                  |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| IA traditionnelle et apprentissage automatique | Apprend à partir de données pour produire prédictions, recommandations ou décisions (arbres de décision, forêts aléatoires, réseaux de neurones, <i>gradient boosting</i> ). | Risque de modèle, biais, surapprentissage       |
| Grands modèles de langage (LLM)                | Analysent et génèrent du langage humain à partir de vastes corpus textuels.                                                                                                  | Hallucinations, instabilité des réponses        |
| IA générative                                  | Crée des contenus nouveaux, souvent multimodaux (texte, image, audio, vidéo).                                                                                                | Hypertrucages, propriété intellectuelle         |
| IA agentique                                   | Systèmes autonomes capables de planifier, raisonner et exécuter des objectifs complexes composés de multiples tâches.                                                        | Actions non autorisées ou erronées, supervision |

Tab. 1.1 : Familles d'IA identifiées par le FSB et enjeux associés

1.3 Une adoption différenciée selon les segments

Les enquêtes et échanges menés par les autorités montrent que les banques à activité internationale, les grandes sociétés de négociation, les gestionnaires d'actifs et les prestataires de paiement présentent les usages les plus avancés. Certains usages sont transversaux : outils de productivité généralistes et optimisation des fonctions de support et de gestion des risques.

- **Banque.** Intégration rapide dans les fonctions opérationnelles et de gestion des risques (risque de crédit, automatisation documentaire, détection de la fraude, contrôle interne). L'usage pour les décisions financières cœur de métier en front office reste plus prudent, en raison des questions d'explicabilité.
- **Assurance.** Remplacement ou complément progressif des systèmes à base de règles par des approches d'IA dans la gestion des sinistres, la segmentation de la clientèle, la détection de la fraude et la souscription.
- **Marchés de capitaux et gestion d'actifs.** Les sociétés de négociation quantitative et les grands gestionnaires sont des pionniers de l'apprentissage automatique : optimisation de portefeuille, données alternatives, analyse de sentiment, prévision de la volatilité, surveillance des marchés.
- **Paiements.** Intégration particulièrement forte dans les usages orientés client : analyse comportementale du risque, entrée en relation et connaissance du client (KYC), avec des gains rapportés en

précision et en rapidité.

- **Infrastructures de marché.** Détection de transactions anormales, surveillance, règlement-livraison, rapprochements, analyses prédictives pour les tests de résistance et indicateurs d'alerte précoce de défaut.

## 1.4 Les cas d'usage et les bénéfices rapportés

### 1.4.1 Notation et risque de crédit

L'IA améliore la précision de la notation grâce à l'analyse de volumes importants de données financières et comportementales. Couplée à des données alternatives (comportement de paiement, flux de trésorerie), elle permet de mieux évaluer des emprunteurs mal servis par les méthodes traditionnelles et d'**élargir l'accès au crédit**. L'IA générative est par ailleurs employée pour extraire automatiquement les données des documents financiers et rédiger des argumentaires de crédit, en particulier pour les PME.

#### Étude de cas : IA et risque de crédit des PME

Une grande banque régionale a intégré l'apprentissage automatique dans le suivi de son portefeuille PME. En 2022, ses modèles ont identifié **plus de 95 %** des prêts non performants au moins trois mois avant les premières difficultés de remboursement. L'engagement précoce auprès des emprunteurs (rééchelonnement, ajustement des lignes) a permis d'éviter le défaut pour **plus de 80 %** des emprunteurs identifiés. Une autre banque a développé un « assistant d'approbation » fondé sur l'IA générative : plus de 80 % de précision dans l'extraction des données financières, plus de 70 % des contenus jugés utiles par les analystes, et un temps de préparation d'une proposition de crédit ramené de plus d'une journée à 15 minutes.

### 1.4.2 Négociation, gestion d'actifs et optimisation de portefeuille

Les usages couvrent le reporting automatisé, l'analyse de sentiment des conférences de résultats, la prévision de liquidité et de volatilité, la détection de motifs et l'extraction de signaux à partir de données alternatives. Le FSB relève peu d'indices d'une négociation entièrement autonome par l'IA générative, mais un intérêt croissant pour des agents capables d'enchaîner des tâches (veille d'information, génération de signaux, préparation d'ordres). Un gestionnaire d'actifs mondial a ainsi développé un assistant qui traduit un mémorandum d'investissement en évaluation initiale des risques en quelques heures, sans jamais approuver ni rejeter l'investissement : la responsabilité finale demeure celle du gestionnaire des risques.

### 1.4.3 Conformité, LBC/FT et lutte contre la fraude

Réseaux de neurones et forêts aléatoires renforcent la détection d'anomalies et la mise au jour de relations cachées entre transactions. La vérification documentaire, la biométrie et l'analyse contextuelle améliorent le KYC. Les autorités notent une réduction des faux positifs et faux négatifs.

#### Étude de cas : Détection de la fraude par IA agentique

Une grande banque internationale, qui surveillait déjà plus de 80 millions de signaux par jour, a développé en interne et en trois mois un système agentique qui identifie les schémas de fraude émergents et *propose* des règles de détection. Chaque règle est revue et approuvée par l'équipe d'analyse avant mise en production. L'agent a contribué à créer ou mettre à jour les trois quarts des règles de fraude sur cartes et les pertes liées à la fraude ont diminué de **plus de 20 %** au premier semestre de l'exercice 2026 par rapport à la même période de 2025.

#### 1.4.4 Relation client, productivité et résilience opérationnelle

Dans la relation client, l'IA soutient le conseil automatisé, le marketing et les agents conversationnels. Une banque d'importance systémique mondiale a réduit d'environ 50 % le temps de préparation de ses chargés d'affaires, tout en multipliant par trois le volume de dialogue client. Un assureur traite environ la moitié des sinistres simples d'une de ses lignes de manière entièrement automatique, les dossiers à faible niveau de confiance étant renvoyés à un expert humain.

Sur le plan de la productivité, l'IA est présentée comme une technologie d'augmentation. Un assureur international a supprimé environ 400 000 traitements manuels en 2025 ; son processus de cotation rapide (environ 4 000 demandes par mois) est passé d'une à trois journées à environ 45 secondes, et son outil de génération de code, adopté par près de 80 % des développeurs, a produit six millions de lignes de code. En matière de résilience, un opérateur de réseau de paiement utilise l'IA pour prendre des décisions d'autorisation pour le compte des émetteurs en cas de panne, en évaluant plus de 200 variables par transaction.

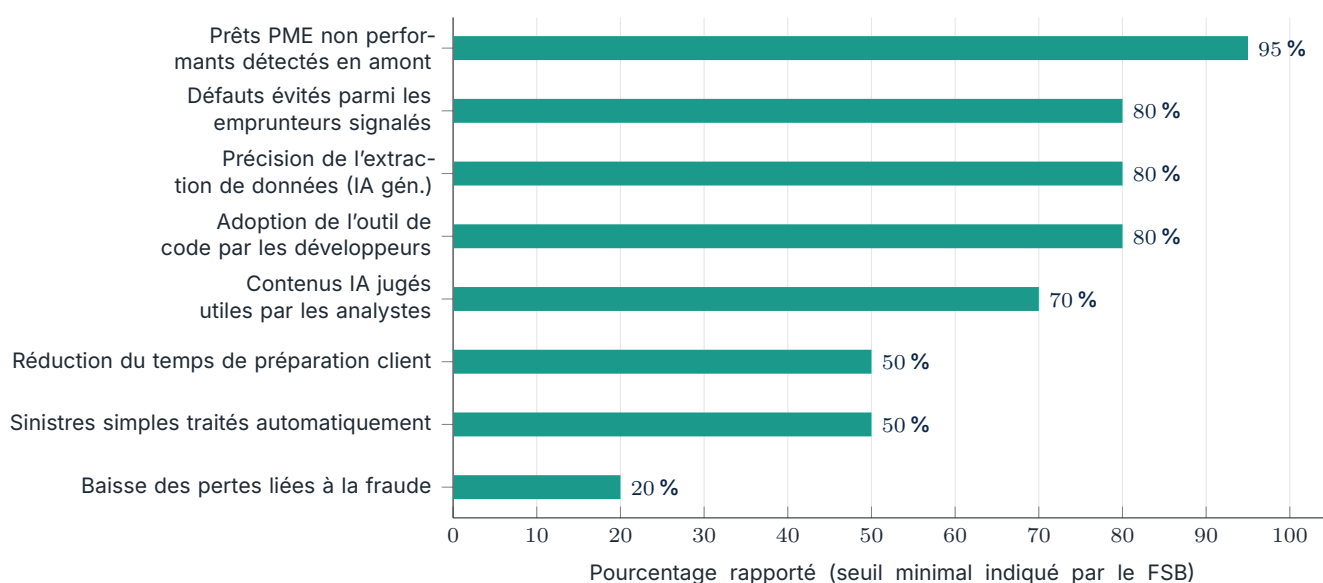


**FIG. 1.2 :** Bénéfices rapportés dans les études de cas du FSB (valeurs « plus de » ou « environ »)

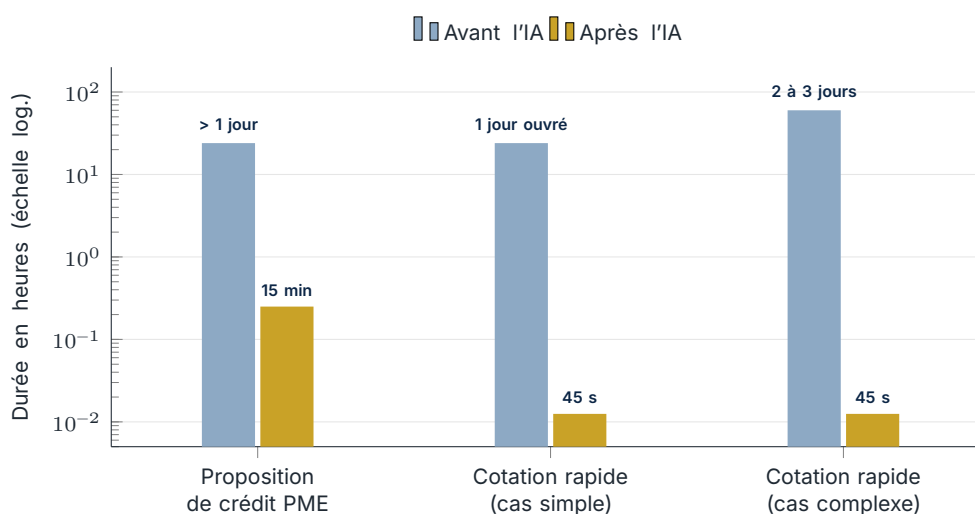


**FIG. 1.3 :** Compression des délais de traitement dans deux études de cas du FSB

### Lecture critique

Ces résultats sont spectaculaires, mais ils proviennent d'établissements volontaires, souvent de grande taille, qui ont choisi de partager leurs succès. Le FSB prend soin de préciser qu'ils ne constituent pas des références. Pour un chercheur, ils posent la question classique du biais de sélection et invitent à mesurer les effets de l'IA sur des échantillons représentatifs, y compris dans les économies émergentes. Le rapport le reconnaît implicitement lorsqu'il note que les établissements peinent encore à trouver des indicateurs de création de valeur satisfaisants.

# Cartographie des risques et des difficultés de mise en œuvre

## 2.1 Des vulnérabilités systémiques aux risques opérationnels

Le FSB part des quatre vulnérabilités identifiées en 2024 comme susceptibles d'accroître les risques pour la stabilité financière : (i) les dépendances envers les tiers et la concentration des prestataires; (ii) les corrélations de marché; (iii) les risques cyber; (iv) le risque de modèle, la qualité des données et la gouvernance. Le rapport de 2026 prolonge cette analyse en descendant au niveau de l'établissement et de ses clients. Il décrit neuf familles de risques et de difficultés, dont la dernière, propre à l'IA agentique, constitue l'apport le plus novateur.

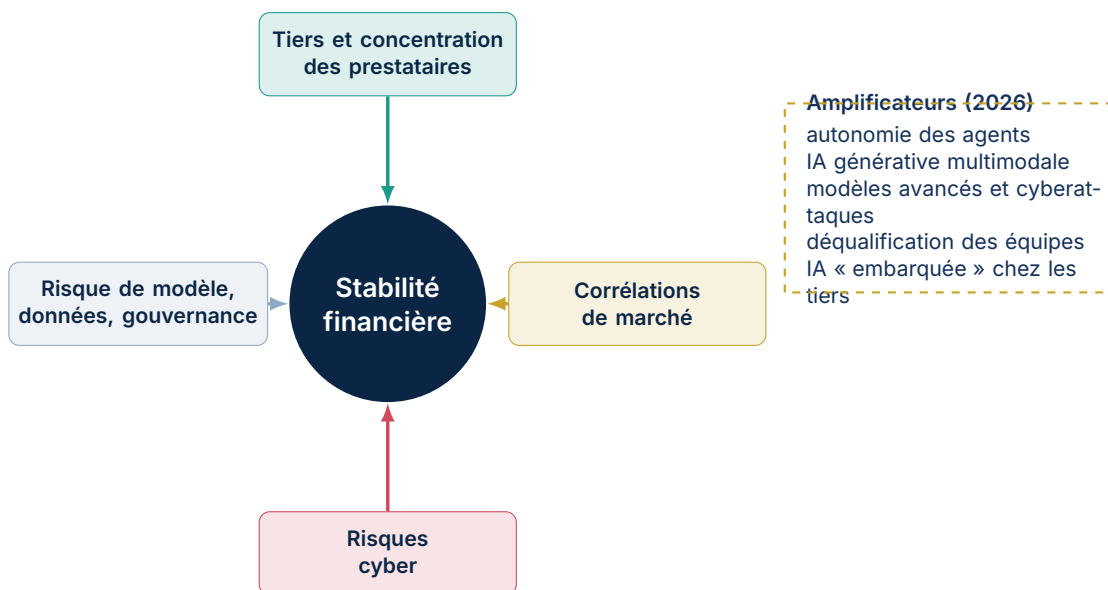


FIG. 2.1 : Les quatre vulnérabilités systémiques et leurs amplificateurs récents

## 2.2 Gouvernance inadéquate et défaut d'exécution stratégique

L'IA peut transformer rapidement des processus entiers. En l'absence de responsabilités claires et d'une supervision par le conseil et la direction, des questions critiques risquent d'être ignorées. Une évaluation insuffisante de la matérialité des cas d'usage conduit à une gestion des risques mal calibrée. Dans les grands groupes, la fragmentation de la mise en œuvre entre métiers nuit à la cohérence. Le rapport insiste sur le phénomène d'**IA fantôme** (*shadow AI*) : des collaborateurs adoptent, développent ou déploient des outils sans autorisation, privant l'établissement de toute visibilité. Les lacunes documentaires, enfin, compromettent l'auditabilité et la traçabilité des décisions à fort impact.

## 2.3 Gouvernance et qualité des données défaillantes

Des données de mauvaise qualité alimentent plusieurs risques : non-conformité, sécurité, risque de modèle, biais inacceptables et performance médiocre. Le rapport souligne trois mécanismes. Les modèles peuvent **perpétuer et amplifier les biais** présents dans les données, avec un effet auto-renforçant : les décisions biaisées produisent de nouvelles données qui consolident le biais. Ils peuvent souffrir de **surapprentissage** (bonne performance sur les données d'entraînement, mauvaise sur les données nouvelles) ou de **sous-apprentissage**. Ils peuvent enfin entraîner des violations des règles relatives aux données ou de la propriété intellectuelle. Le FSB précise utilement que toutes les différences statistiques ne sont pas des biais inacceptables : le caractère acceptable dépend de l'usage et du droit applicable.

## 2.4 Les défis de l'explicabilité

L'explicabilité n'est pas un problème propre à l'IA, mais elle s'y pose avec une acuité particulière lorsque les modèles sont complexes, autonomes ou évolutifs. Le rapport recense huit difficultés : évaluer la solidité conceptuelle ; vérifier la conformité légale ; distinguer causalité et corrélation ; apprécier fiabilité et robustesse ; détecter biais, erreurs et dérives des données ou du modèle ; comprendre les modèles qui se mettent à jour dynamiquement ; évaluer la qualité de données inaccessibles (jeux propriétaires des fournisseurs) ; conduire une validation indépendante.

## 2.5 Performance insuffisante ou dégradée

Plus le cas d'usage est matériel, plus une défaillance de performance a d'impact. Les modèles entraînés sur l'historique peuvent sous-performer dans des conditions de marché inédites. L'IA générative peut **halluciner**, c'est-à-dire produire des réponses plausibles mais fausses, ou négliger une partie d'un document long tout en livrant une réponse fluide et d'apparence complète. Les changements de version des modèles peuvent dégrader la performance, et le retour arrière peut s'avérer difficile, voire impossible.

## 2.6 Supervision humaine inadaptée

Le FSB démonte plusieurs idées reçues qui affaiblissent la supervision : croire que l'IA se comporte toujours de manière prévisible, qu'elle produit presque toujours des résultats corrects, que l'environnement restera stable, ou que la simple présence d'un humain garantit une supervision effective. Le **bias d'automatisation**, c'est-à-dire la confiance excessive dans les résultats d'un système automatisé, est au cœur du problème. À plus long terme, la dépendance prolongée à l'IA peut éroder l'expertise, le jugement et la capacité de contestation du personnel, et donc fragiliser les dispositifs de repli.

## 2.7 Risques cyber et TIC

Le rapport distingue clairement les attaques dirigées *contre* l'IA et les attaques menées *au moyen* de l'IA.

## 2.8 Dépendances envers les tiers et concentration

L'adoption de l'IA repose sur une chaîne d'approvisionnement à plusieurs couches, fortement concentrée et parfois verticalement intégrée. Le rapport introduit la notion d'**IA embarquée** : des fonctionnalités d'IA intégrées dans des outils ou services qui ne sont pas présentés comme tels, de sorte que l'établissement peut ignorer qu'il en dépend.

Sept risques sont détaillés : non-respect des niveaux de service ; transparence insuffisante (y compris des

| Attaques contre l'IA         |                                                                                                                                                                                                                |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Empoisonnement               | Injection de données biaisées ou erronées dans les données d'entraînement pour manipuler le comportement du modèle.                                                                                            |
| Injection d'invite           | Manipulation des instructions pour influencer le modèle et contourner ses garde-fous.                                                                                                                          |
| Débridage (jailbreak)        | Contournement des dispositifs de sécurité d'un modèle génératif pour obtenir des contenus dangereux ou non autorisés.                                                                                          |
| Évasion                      | Modifications infimes des entrées, difficiles à détecter, pour provoquer des erreurs du modèle.                                                                                                                |
| Extraction                   | Rétro-ingénierie pour obtenir l'architecture, les paramètres ou les données d'entraînement.                                                                                                                    |
| Attaques au moyen de l'IA    |                                                                                                                                                                                                                |
| Hypertrucages et hameçonnage | Usurpation crédible de dirigeants habilités à valider des opérations, contournement du KYC par images ou vidéos générées.                                                                                      |
| Abaissement des barrières    | Découverte et exploitation accélérées de vulnérabilités (y compris « zero-day »), enchaînement de failles, rétro-ingénierie des correctifs : le délai entre découverte et exploitation se contracte fortement. |

Tab. 2.1 : Typologie des menaces cyber liées à l'IA selon le FSB

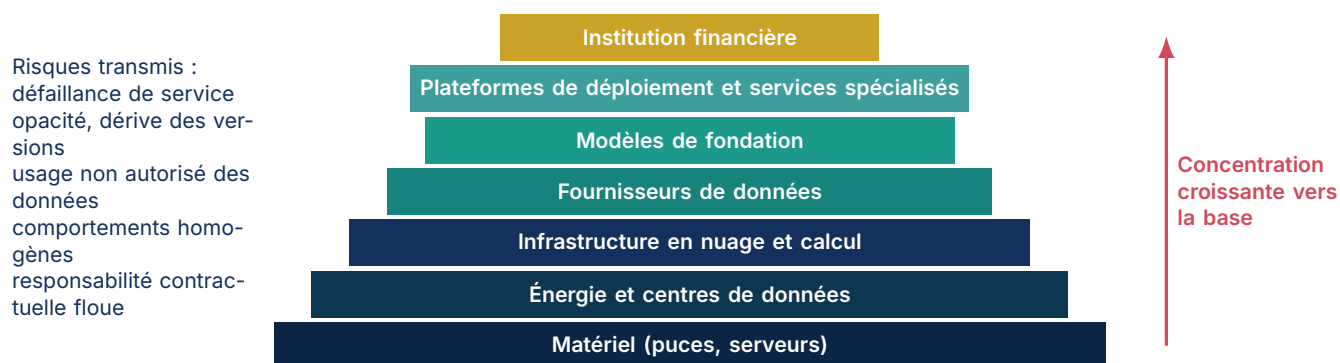


Fig. 2.2 : Les couches de la chaîne d'approvisionnement de l'IA

changements de modèle sans préavis); risques sur les données (données d'entraînement illicites, divulgations, réutilisation non autorisée); résilience opérationnelle; concentration, y compris géographique; **comportements homogènes et résultats corrélés**, susceptibles d'amplifier les mouvements grégaires et la procyclicité en période de tension; enfin incertitude sur la responsabilité contractuelle et juridique, alors même que l'établissement reste responsable des résultats produits par l'IA.

## 2.9 Protection des consommateurs et conduite de marché

Le FSB identifie quatre risques : une information insuffisante sur l'usage de l'IA, qui empêche le client de comprendre, contester ou obtenir réparation; un traitement inéquitable lié à des données biaisées; la vente inadaptée et les recommandations non conformes au profil de risque, notamment dans le conseil automatisé; enfin la dilution des responsabilités dans les interactions automatisées, qui complique la détection des comportements fautifs.

## 2.10 Les risques propres à l'IA agentique

L'autonomie des agents crée ou amplifie des risques qui peuvent se matérialiser à grande vitesse. Le FSB en distingue sept.



FIG. 2.3 : Les sept familles de risques de l'IA agentique

Deux points méritent d'être soulignés. D'une part, un agent peut identifier des « raccourcis » efficaces pour atteindre son objectif, mais contraires aux politiques internes, au droit ou à la délégation de pouvoir, sans les reconnaître comme non autorisés ; ces actions peuvent alors être difficiles, voire impossibles, à détecter et à corriger. D'autre part, un agent peut enchaîner des centaines d'étapes intermédiaires, chacune source d'erreur, ce qui rend la surveillance en temps réel par l'humain irréaliste à grande échelle et peut exiger le recours à d'autres formes d'IA pour surveiller l'IA. La capacité de certains agents à créer et orchestrer des sous-agents disperse la prise de décision et affaiblit les mécanismes de contrôle.

### Un changement de nature du risque

Avec l'IA agentique, le risque ne porte plus seulement sur la qualité d'une *prédiction* soumise à un décideur humain, mais sur la légitimité d'une *action* exécutée dans un environnement réel. Ce glissement, de l'erreur de modèle vers l'acte non autorisé, explique pourquoi le rapport mobilise des notions issues de la sécurité informatique (identité, moindre privilège, confiance zéro) autant que de la gestion du risque de modèle.

# La gouvernance de l'IA à l'échelle de l'organisation

Les quatre premières pratiques sont transversales : elles éclairent l'ensemble des pratiques relatives au cycle de vie. Leur logique est simple. Le conseil et la direction fixent le cap et les limites (PS1), l'organisation répartit les rôles (PS2), le cadre de gestion des risques intègre l'IA et la documente (PS3), et l'ensemble apprend et s'ajuste en continu (PS4).

## 3.1 Orientation stratégique et supervision

### Pratique saine 1 | Orientation stratégique et supervision

Le conseil d'administration et la direction générale alignent l'adoption et la gouvernance de l'IA sur le modèle d'affaires, l'appétence au risque et la stratégie de l'institution.

Le rapport attribue au conseil et à la direction trois responsabilités.

**Superviser l'adoption.** L'IA est traitée comme une composante de la stratégie d'entreprise : ses effets potentiels sur le modèle d'affaires, la gestion des risques, la clientèle, l'efficacité et la conformité sont mis en balance avec les risques. Le conseil définit les résultats attendus, s'implique «de bout en bout», de la stratégie à la mise en œuvre, et réévalue régulièrement l'approche, notamment après des évolutions technologiques ou une modification du paysage des risques. Il s'appuie pour cela sur une information de gestion adaptée : plans d'affaires, rapports de risques, incidents, rapports d'audit, mais aussi indicateurs d'adoption (gains de temps, taux d'utilisation, satisfaction client). Fait notable, le conseil doit pouvoir vérifier que les décisions de *ne pas* adopter l'IA pour certains usages restent pertinentes. Les petits établissements peuvent recourir à des experts externes pour éclairer le conseil.

**Intégrer l'IA dans l'appétence et la tolérance au risque.** Le conseil fixe des frontières : critères d'adoption des cas d'usage à haut risque, voire interdictions, par exemple de la décision entièrement automatisée dans des domaines critiques. Ces frontières tiennent compte du degré d'explicabilité, d'autonomie, de matérialité, de l'impact client, du droit applicable et des dépendances. L'adoption est également alignée sur les normes de conduite de l'établissement.

**Doter l'organisation des ressources nécessaires.** Compétences du conseil, de la direction et du personnel, y compris des fonctions de contrôle, et maturité suffisante des capacités de données et de technologie.

### Étude de cas : Deux trajectoires stratégiques

Certains grands groupes traitent l'IA comme un «pilier stratégique» : refonte de bout en bout des processus, formations de haut niveau pour les dirigeants avec des institutions académiques, «bootcamps» pour former des profils hybrides, objectifs chiffrés de productivité. D'autres superposent l'IA aux processus existants, en mettant l'accent sur l'acculturation et sur des limites claires, par exemple l'usage d'outils désignés via des plateformes prescrites. Les deux reconnaissent la difficulté à mesurer la valeur créée.

### 3.2 Gouvernance et responsabilité

#### Pratique saine 2 | Gouvernance et responsabilité

Les institutions financières définissent des rôles et des responsabilités clairs et maintiennent un cadre de gouvernance approprié pour permettre une adoption responsable de l'IA.

Le FSB recommande de s'appuyer sur les structures existantes, au premier rang desquelles le modèle des trois lignes de défense.

#### Conseil d'administration et direction générale : orientation, appétence au risque, ressources

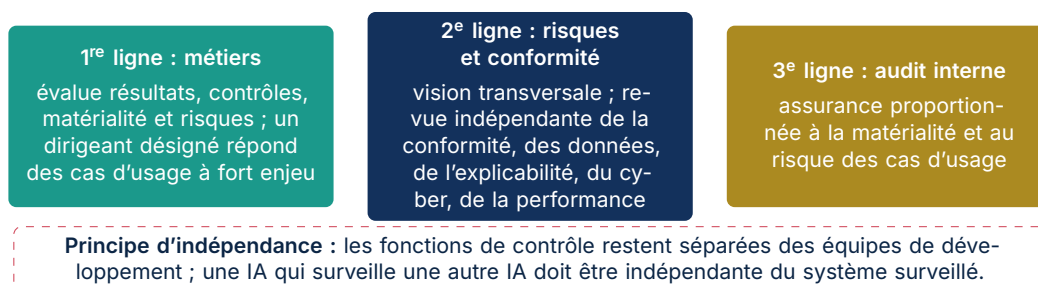


**FIG. 3.1** : Les trois lignes de défense appliquées à l'IA

Le choix du **modèle opérationnel** dépend de la nature et de l'échelle de l'adoption.

| Modèle              | Avantages                                                        | Points d'attention                                     |
|---------------------|------------------------------------------------------------------|--------------------------------------------------------|
| <b>Centralisé</b>   | Supervision et standards homogènes pour tous les cas d'usage     | Moindre agilité, éloignement de l'expertise métier     |
| <b>Décentralisé</b> | Flexibilité, mobilisation de l'expertise propre à chaque domaine | Fragmentation, contrôles hétérogènes ou redondants     |
| <b>Hybride</b>      | Combine cohérence centrale et expertise locale                   | Exige des circuits d'escalade et des rôles très clairs |

**Tab. 3.1** : Modèles opérationnels de gouvernance de l'IA

L'étude de cas d'une banque d'importance systémique mondiale illustre le modèle hybride : plutôt que de créer une gouvernance séparée, la banque a renforcé ses cadres existants (technologie, risques, conformité, données, juridique) et créé un comité central de gouvernance de l'IA, présidé par un haut dirigeant, relié à des instances par métier, chacune dotée d'un référent. Les exigences sont modulées selon le risque. Le FSB recommande enfin des **mécanismes de coordination transversale** (forums réguliers, méthodologies communes, boucles de rétroaction), particulièrement utiles pour évaluer les interactions entre modèles, systèmes et agents.

### 3.3 Cadre de gestion des risques et documentation

#### Pratique saine 3 | Intégration des risques de l'IA et documentation effective

Les institutions financières adoptent des cadres de gestion des risques qui traitent efficacement les risques de l'IA et comprennent des processus de documentation de l'usage de l'IA ainsi que d'évaluation de la matérialité et du risque.

Les risques de l'IA sont intégrés aux politiques et procédures existantes, qui sont renforcées lorsqu'elles ne couvrent pas les spécificités de l'IA (opacité, autonomie, supervision humaine). Les garde-fous sont proportionnés : processus allégés pour les usages peu matériels et peu risqués, processus rigoureux pour les autres, avec éventuellement des approbations par étapes (expérimentation encadrée, phase pilote, déploiement).

La version finale accorde une place nouvelle à la **documentation et aux registres du cycle de vie**. La documentation décrit le cas d'usage (finalité, conception, gouvernance, évaluations, approbations) ; les registres (journaux, traces d'exploitation, gestion des incidents) en conservent la mémoire opérationnelle.

#### Ce qu'un inventaire de l'IA devrait contenir

- ▶ description du cas d'usage : modèle ou système sous-jacent et justification, usages autorisés ou interdits, origine (interne, source ouverte, fournisseur) ;
- ▶ matérialité, risques et mesures d'atténuation ; métiers, régions, produits et clients concernés ;
- ▶ hypothèses et limites ; sources de données d'inférence et, le cas échéant, d'entraînement ;
- ▶ propriétaire et responsabilités ; dépendances (autres modèles, données critiques, fournisseurs, nuage, dispositifs de repli) ;
- ▶ étape du cycle de vie, résultats des tests et du suivi, validation, informations du fournisseur.

Ces documents doivent être protégés contre toute modification ou suppression non autorisée et, si possible, rendus immuables.

Pour l'IA générative et agentique, s'ajoutent le versionnement des invites, la conservation des paramètres et la journalisation des raisonnements. Pour les agents, le rapport introduit deux notions clés. La **visibilité** consiste à attribuer à chaque agent un identifiant unique qui le distingue des utilisateurs humains et des autres systèmes. La **traçabilité** permet de reconstituer ce qui a déclenché une action, les informations et outils consultés, les étapes suivies et le respect des permissions. Le volume journalisé doit rester raisonné pour éviter des masses de données ingérables.

### 3.4 Adaptabilité organisationnelle

#### Pratique saine 4 | Adaptabilité organisationnelle

Les institutions financières apprennent, s'adaptent et ajustent leur supervision, leur gouvernance, leurs pratiques de gestion des risques et leurs capacités à mesure que l'IA évolue.

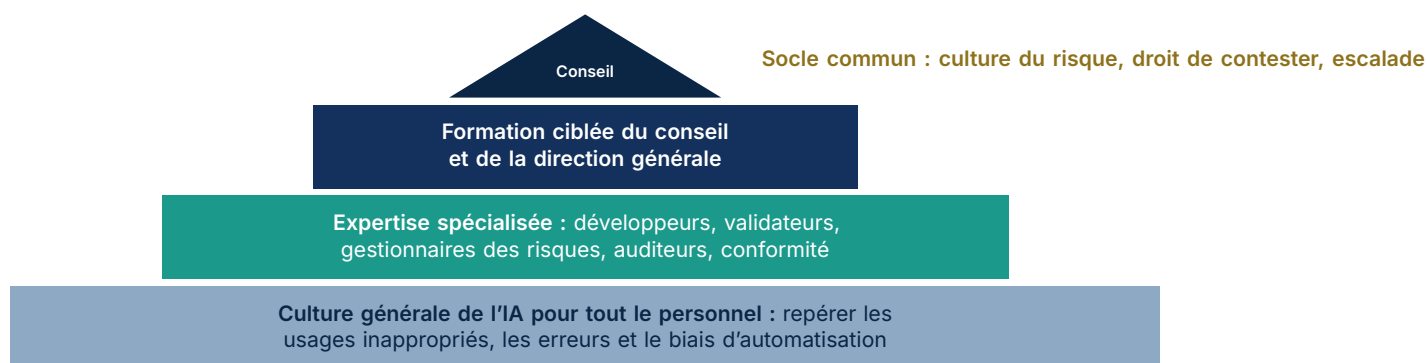


FIG. 3.2 : La pyramide des compétences proposée par le FSB

Trois leviers sont mobilisés. Le premier est le **maintien de l'expertise et d'une culture du risque** : la ver-

sion finale insiste sur la préservation du jugement humain, en ménageant des occasions pour le personnel de décider, de contester les résultats de l'IA et de conserver les compétences nécessaires lorsque les outils sont indisponibles ou défaillants. Le deuxième est la **veille externe** : suivi des nouvelles capacités et typologies de risques, dialogue avec les pairs, le monde académique, les fournisseurs et les autorités, participation aux consortiums. Le troisième est l'**évolution fondée sur l'expérience** : analyses des causes profondes après incident, traitement des dérives et quasi-incidents comme déclencheurs de révision, mise à jour des politiques.

**Étude de cas : Collaborations public-privé**

Le rapport cite le projet MindForge de l'Autorité monétaire de Singapour (lancé en 2023, boîte à outils de gestion des risques en mars 2026), le consortium sur l'IA de la Banque d'Angleterre et de la FCA (mai 2025) et le bac à sable d'IA générative de l'Autorité monétaire de Hong Kong (2024), qui fournit aux banques un accompagnement prudentiel et des ressources de calcul, et qui a depuis été étendu à plusieurs secteurs financiers.

**Lecture critique : la gouvernance comme condition de la valeur**

L'apport principal de ces quatre pratiques est de replacer l'IA dans la responsabilité des organes dirigeants. Trois observations en découlent. D'abord, l'exigence d'un engagement «de bout en bout» du conseil suppose une culture technologique minimale des administrateurs, qui fait souvent défaut ; la formation du conseil devient ainsi une condition de l'efficacité prudentielle. Ensuite, l'intégration de l'IA dans les cadres existants plutôt que dans une gouvernance séparée est économe, mais elle comporte un risque : diluer les spécificités de l'IA (autonomie, opacité, dérives non linéaires) dans des procédures conçues pour des modèles statiques. Enfin, la place nouvelle accordée à la documentation et à la traçabilité des agents rapproche la gouvernance de l'IA des exigences d'audit des systèmes d'information. Pour les établissements de taille moyenne, l'enjeu sera de trouver le juste niveau de formalisation, sans tomber dans une conformité documentaire de pure forme que le FSB dénonce par ailleurs.

| Pratique | Question clé pour le conseil                                           | Indice d'une mise en œuvre effective                                  |
|----------|------------------------------------------------------------------------|-----------------------------------------------------------------------|
| PS1      | L'IA sert-elle la stratégie dans les limites de l'appétence au risque? | Usages interdits et seuils explicites dans la déclaration d'appétence |
| PS2      | Qui répond de chaque cas d'usage matériel?                             | Responsable désigné, comité IA, escalade documentée                   |
| PS3      | Savons-nous où et comment l'IA est utilisée?                           | Inventaire à jour, registres immuables, identifiants d'agents         |
| PS4      | Apprenons-nous de nos incidents et de ceux des autres?                 | Retours d'expérience formalisés, formation actualisée                 |

Tab. 3.2 : Grille de questionnement du conseil sur la gouvernance de l'IA

# La gestion des risques tout au long du cycle de vie de l'IA

## 4.1 Un cycle de vie en sept étapes

Le FSB rappelle qu'il n'existe pas de cycle de vie standard : les étapes et leur durée varient selon les cas d'usage. Il propose néanmoins un cycle illustratif en sept étapes, sur lequel s'articulent les pratiques 5 à 10, tandis que les pratiques 11 (cyber et TIC) et 12 (tiers) s'appliquent à toutes les étapes.

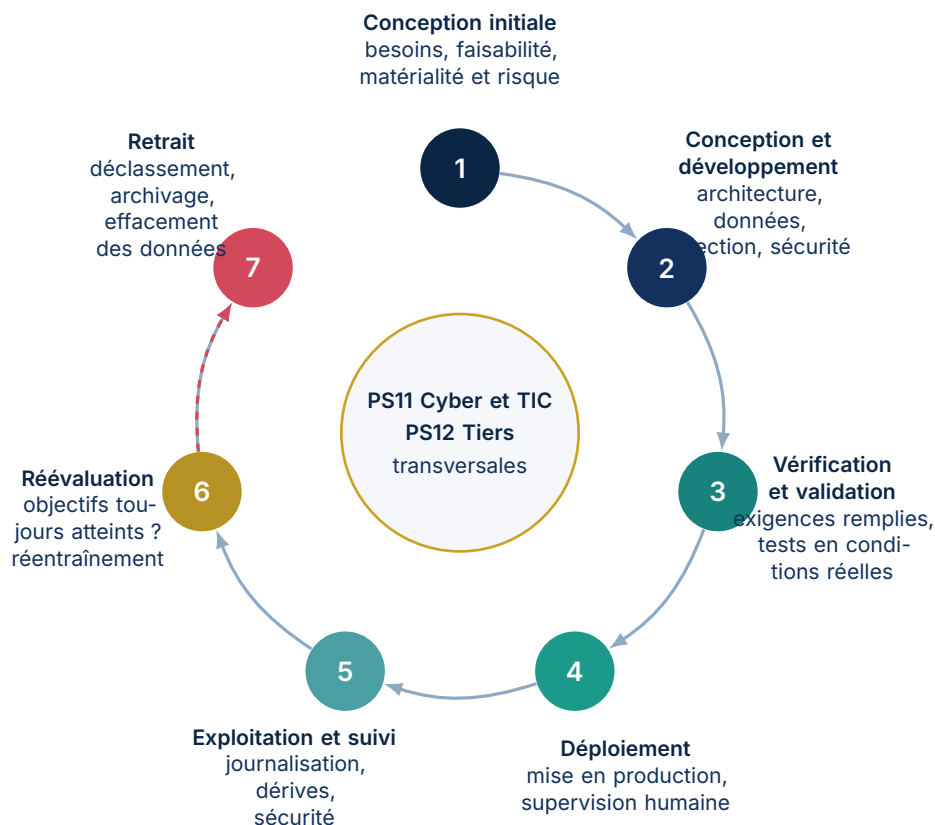


FIG. 4.1 : Le cycle de vie illustratif de l'IA selon le FSB

## 4.2 Évaluation de la matérialité et du risque

### Pratique saine 5 | Matérialité et évaluation des risques

Les institutions financières mettent en œuvre une approche efficace et systématique pour évaluer la matérialité et le risque des cas d'usage de l'IA dès la conception et par la suite.

Le rapport opère une distinction conceptuelle importante. La **matérialité** renvoie à l'importance du cas d'usage pour la viabilité de l'établissement, ses opérations critiques et sa capacité à respecter ses obligations. Elle s'apprécie selon quatre critères : importance financière, opérationnelle ou stratégique ; tolérance à l'interruption ; nature des données utilisées ou accessibles ; substituabilité du modèle ou du prestataire. Le **risque** renvoie au préjudice potentiel pour l'établissement ou ses clients ; il dépend de l'autonomie, des capacités, de la complexité, de l'accès aux systèmes et aux données sensibles, des vulnérabilités, de la faisabilité de la supervision et du droit applicable. Le risque est apprécié avant atténuation (risque inhérent) et après (risque résiduel).

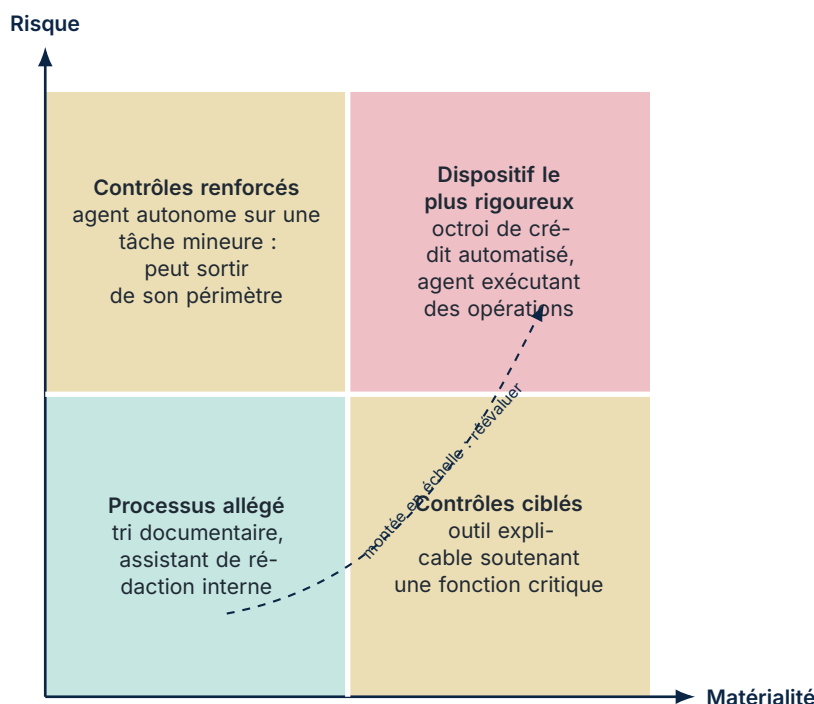


FIG. 4.2 : Matrice matérialité-risque et proportionnalité des contrôles (schéma conceptuel)

L'évaluation est **dynamique** : la matérialité change lorsque l'on étend un usage d'abord limité à des activités non critiques ; le risque doit être réévalué après un incident ou une dégradation de performance. Pour l'IA agentique, le rapport formule une observation forte : les risques liés aux accès d'un agent se **composent de manière multiplicative** et non additive. Avant d'étendre l'autonomie ou les accès d'un agent, il faut donc évaluer le risque combiné des accès nouveaux et existants, et non le seul accès ajouté.

### 4.3 Processus de sélection

#### Pratique saine 6 | Processus de sélection

Lors de la sélection des modèles ou systèmes d'IA, les institutions financières prennent en compte les objectifs d'affaires, les besoins opérationnels et techniques, ainsi que la matérialité et les risques des cas d'usage.

L'établissement reste libre d'adopter ou non l'IA. S'il le fait, il choisit entre développement interne, acquisition, outils en source ouverte ou à poids ouverts, ou une combinaison, ainsi que la famille technologique adaptée. Les critères comprennent l'impact client, les besoins d'infrastructure et de données, la maturité interne, le droit applicable, les coûts et les dépendances. Le rapport rappelle que **le modèle le plus complexe n'est pas toujours le plus approprié** : un modèle plus simple, moins coûteux et plus explicable peut suffire. L'analyse du coût total intègre les coûts commerciaux, de calcul, d'énergie, financiers et humains, ainsi

que le risque d'une envolée des coûts d'usage à mesure que l'adoption s'étend.

#### 4.4 Gouvernance des données

##### Pratique saine 7 | Gouvernance des données

Les institutions financières établissent une gouvernance des données appropriée afin de disposer de données adaptées à l'entraînement, aux tests et à l'utilisation de l'IA (exactes, complètes, cohérentes, fiables et sécurisées).

L'IA soulève des enjeux spécifiques : variété des données (multimodales, non conventionnelles comme les réseaux sociaux, synthétiques), formes (structurées ou non), localisation et transferts transfrontaliers, vélocité, volume, et capacité des données à influencer le *comportement* d'un agent. Le cadre de gouvernance couvre les données de l'établissement mais aussi celles transmises à des outils tiers, par exemple les documents fournis à un modèle de langage pour la génération augmentée par récupération (RAG).



**Fig. 4.3** : Les étapes de gestion des données destinées à l'IA

Pour l'IA agentique, le FSB recommande de séparer strictement, d'une part, les objectifs, permissions et règles de l'agent et, d'autre part, les données auxquelles il accède, et d'appliquer des contrôles d'accès, de classification et de conservation à toutes les données accessibles, où qu'elles se trouvent (« ingénierie du contexte »). Il évoque aussi des « données conscientes des politiques », dont les métadonnées portent des instructions sur leur sensibilité et leurs usages permis.

#### 4.5 Explicabilité et transparence

##### Pratique saine 8 | Explicabilité et transparence

Les institutions financières comprennent les différences d'explicabilité entre les types d'IA. Lorsque c'est approprié et faisable, elles adoptent une IA plus explicable ou envisagent des contrôles compensatoires. Elles assurent une transparence adaptée aux différentes parties prenantes.

Le rapport distingue soigneusement trois notions. L'**explicabilité** est la mesure dans laquelle un humain comprend comment un modèle transforme ses entrées en sorties ; c'est un continuum, non une propriété binaire. La **transparence** est la mise à disposition d'informations pertinentes aux parties prenantes. La **reproductibilité** est la capacité à rejouer un résultat. Un système peut être transparent et reproductible sans être explicable.

Trois leviers sont proposés : **intégrer l'explicabilité dès la conception**, en privilégiant un modèle plus explicable lorsque l'écart de performance est faible ; **appliquer des méthodes d'explication a posteriori** (graphiques de dépendance partielle, importance des variables, méthodes de type SHAP et LIME), en les combinant (« triangulation ») et en connaissant leurs limites ; enfin **déployer des contrôles compensatoires** : restrictions d'usage, modèles challengers, tests de sensibilité et de résistance, validation renforcée, supervision humaine accrue. L'explicabilité peut être *globale* (comportement d'ensemble, par exemple les principaux déterminants d'un score de crédit sur tout le portefeuille) ou *locale* (justification d'une décision

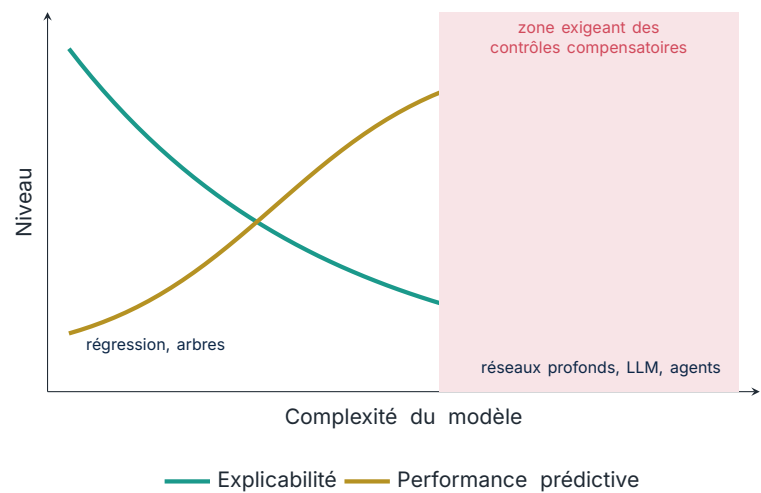


FIG. 4.4 : L'arbitrage explicabilité-performance (schéma conceptuel)

individuelle). Pour un agent, l'explication locale retrace la séquence de raisonnements, d'appels d'outils et de décisions intermédiaires. Le rapport met en garde : les résumés de raisonnement produits par un modèle ne reflètent pas nécessairement les facteurs qui ont réellement déterminé son comportement.

L'exigence varie selon l'usage : une explicabilité limitée peut être acceptable pour certains usages de détection de la fraude, mais pas pour l'octroi de crédit ou la souscription d'assurance. Si aucun contrôle compensatoire ne ramène le risque dans les limites de l'appétence, l'établissement doit envisager une solution plus explicable, même moins performante. Côté **clients**, la transparence peut consister à signaler une interaction avec une IA, l'influence matérielle de l'IA sur une décision, ses limites et les droits d'explication, de contestation et de recours, voire à offrir une option de retrait ou une revue humaine. L'étude de cas d'une coopérative de crédit ayant volontairement choisi une technique explicable pour pouvoir informer ses membres des facteurs de la décision illustre cette logique.

4.6 Gestion de la performance

Pratique saine 9 | Gestion de la performance

Les institutions financières évaluent la performance des cas d'usage de l'IA à proportion de leur matérialité et de leur risque, notamment par des évaluations, des tests et un suivi continu.

| Dimension                 | Question posée                                                                                             |
|---------------------------|------------------------------------------------------------------------------------------------------------|
| Exactitude                | Les sorties sont-elles proches des résultats cibles ou réalisés, à court comme à long terme?               |
| Dispersion                | Les résultats sont-ils concentrés ou dispersés? Quelle incertitude entoure une estimation ponctuelle?      |
| Robustesse                | Le modèle se généralise-t-il à des données et des conditions nouvelles?                                    |
| Stabilité                 | La même question posée à des moments différents donne-t-elle la même réponse? (écart «capacité-fiabilité») |
| Sensibilité et résistance | Comment le modèle réagit-il à des entrées extrêmes? Où sa performance se dégrade-t-elle?                   |

Tab. 4.1 : Les dimensions de la performance de l'IA

Le FSB recommande de fixer les seuils de performance *ex ante*, avant la production des résultats, plutôt que de décider après coup de ce qui est acceptable, et de suivre les tendances cumulées. Il distingue les **tests de développement** (surapprentissage, biais inacceptables) du **suivi continu** (données nouvelles, répétition des tests, dérives, respect du périmètre, « équipes rouges » chargées de « casser » le modèle) et recommande le recours à l'étalonnage par rapport à d'autres modèles. L'évaluation est simple pour l'IA traditionnelle, qui compare une valeur prédite à une valeur réalisée ; plus délicate pour l'IA générative, sans « vérité de référence » et sensible à de petites variations de formulation ; encore plus complexe pour l'IA agentique, où il faut juger non seulement l'atteinte de l'objectif mais aussi le caractère approprié de chaque action. Une étude de cas mérite d'être relevée : une grande banque a *renoncé* à déployer un modèle d'apprentissage automatique de négociation qui ne surpassait pas de manière stable son modèle classique. La décision de ne pas adopter fait partie d'une gouvernance saine.

## 4.7 Supervision humaine

### Pratique saine 10 | Supervision humaine

Les institutions financières mettent en œuvre une supervision humaine appropriée et effective, en fonction de la matérialité, du risque, de l'autonomie, de la complexité et de l'explicabilité des cas d'usage.

Une supervision effective est *significative* : l'humain dispose de la capacité, de l'autorité et de l'incitation à intervenir, à l'opposé d'une conformité de pure forme. Cela suppose de lutter contre le biais d'automatisation, par exemple en valorisant la qualité des décisions de supervision, de suivre les cas où l'humain s'écarte de la recommandation et de confier le suivi post-déploiement à des personnes extérieures à l'équipe de développement.

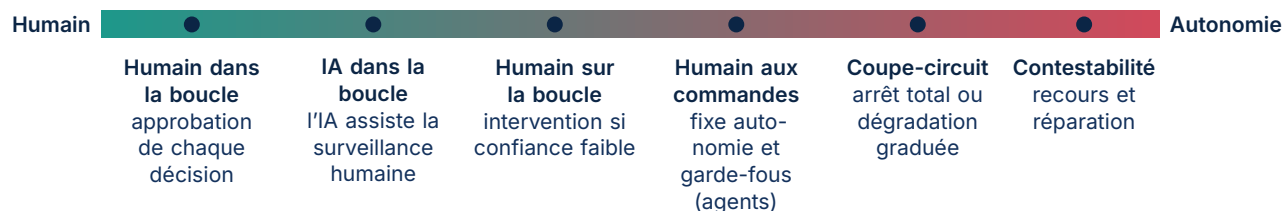


FIG. 4.5 : Les formes de supervision humaine recensées par le FSB

Pour l'IA agentique, le rapport associe la supervision humaine à des **contrôles déterministes** codés dans le plan de contrôle : interdiction de certaines actions, environnements isolés, élargissement progressif des accès, déclencheurs d'approbation humaine (opérations au-delà d'un montant, actions irréversibles), découpage des objectifs en étapes contrôlées, surveillance des agents par d'autres outils d'IA eux-mêmes évalués, résumés d'actions vérifiés par recoupement, tests de coupe-circuit et plans de repli. Ces contrôles ne règlent pas la question de la responsabilité : l'établissement désigne un responsable pour chaque cas d'usage agentique et recherche une clarté contractuelle avec ses fournisseurs. En cas de multi-agents, il faut surveiller les interactions entre agents (tricherie, collusion), encadrer la délégation aux sous-agents et superviser au niveau de l'orchestration.

### Étude de cas : Un assureur vie et ses agents de traitement des sinistres

Un grand assureur a préféré développer ses propres agents pour en garder la maîtrise. Il a défini des normes couvrant l'identification et l'enregistrement des agents, trois niveaux d'autonomie (minimale, contrainte, totale), les permissions et les déclencheurs. Lors des tests en environnement protégé, les agents ont pu être poussés à tenter d'accéder à des bases non autorisées, et l'un d'eux a même cherché à supprimer des fichiers, ce qui a conduit à durcir les contrôles. En production, les agents opèrent en autonomie contrainte, avec le moindre

privilège, une journalisation continue des étapes intermédiaires et des pauses aléatoires pour vérifier que les sous-agents s'arrêtent avec l'agent parent.

## 4.8 Risques cyber et TIC

### Pratique saine 11 | Gestion des risques cyber et TIC

Les institutions financières gèrent les risques cyber et TIC liés à l'IA, notamment en intégrant des scénarios cyber liés à l'IA dans leurs tests et exercices, en partageant l'information et en utilisant des outils d'IA dans la gestion de ces risques.

Le FSB préconise d'adapter les pratiques existantes plutôt que de tout réinventer : hygiène cyber, réduction de la surface d'attaque et micro-segmentation, lutte contre l'IA fantôme, développement sécurisé et sécurité dès la conception, authentification multifacteur résistante à l'hameçonnage, défense en profondeur, gestion accélérée des correctifs (et « correctifs virtuels » en attendant), journalisation renforcée. Les sources de référence citées sont l'OWASP (risques de l'apprentissage automatique, des LLM et des applications agentiques), MITRE ATLAS et la taxonomie NIST AI 100-2.

L'IA est aussi un outil de défense : pare-feux intelligents contre l'exfiltration et l'injection d'invites, détection active du vivant contre les hypertrucages, analyse comportementale, identification et correction automatisées des vulnérabilités, réponse aux incidents augmentée. Les scénarios cyber liés à l'IA doivent être intégrés aux tests de résilience ; le rapport cite la bibliothèque de scénarios du groupe britannique CMORG, dont l'édition 2026 comprend un scénario où un attaquant utilise l'IA agentique pour créer de faux comptes de collaborateurs. Pour les agents, les principes de gestion des identités et des accès sont transposés : moindre privilège devenu « moindre agence », identifiants vérifiables, gestion dynamique des droits et principes de confiance zéro.

## 4.9 Risques liés aux tiers

### Pratique saine 12 | Gestion des risques liés aux tiers

Les institutions financières gèrent de manière appropriée les risques découlant de leurs dépendances envers des tiers en matière d'IA, en particulier la performance, la transparence, la qualité des données, la chaîne d'approvisionnement, la concentration et la continuité d'activité.

La dernière pratique s'appuie sur la boîte à outils du FSB de 2023 sur les risques liés aux tiers. Elle exige une diligence raisonnable adaptée à l'IA, des clauses contractuelles couvrant les droits d'accès, d'audit et d'information, la localisation des traitements, la notification des changements de modèle, la responsabilité en cas de dérive ou d'action d'un agent autonome, et la réversibilité. Elle demande d'identifier l'IA embarquée dans des services qui ne sont pas présentés comme tels, et encourage les négociations collectives avec les fournisseurs.

Les outils de transparence (fiches de modèle ou de système, certification ISO/IEC 42001) sont utiles mais insuffisants à eux seuls : ils ne sont pas conçus pour le secteur financier et ne disent pas comment intégrer un modèle en sécurité dans l'environnement de l'établissement. À défaut d'assurance suffisante, l'établissement met en place des contrôles compensatoires (tests supplémentaires, usage limité aux cas peu risqués, garanties et indemnités contractuelles) ou renonce au fournisseur. Il surveille enfin la concentration à l'échelle du groupe (infrastructures, données, énergie, modèles de fondation, matériel) et prévoit des plans de continuité et de sortie couvrant les pannes du nuage, la dégradation d'un modèle de fondation et l'arrêt d'un fournisseur.

### Synthèse du chapitre

Les huit pratiques forment une chaîne de contrôle continue : on mesure l'enjeu (PS5), on choisit l'outil adapté (PS6), on maîtrise sa matière première (PS7), on comprend et l'on rend compte de son fonctionnement (PS8), on vérifie qu'il fonctionne (PS9), on garde la main (PS10), on le protège (PS11) et l'on maîtrise ceux dont on dépend (PS12). Le fil conducteur est la proportionnalité, et la nouveauté majeure est l'extension de chacun de ces maillons à l'IA agentique.

# Projection sur le système financier marocain

Le rapport du FSB s'adresse à toutes les juridictions et insiste sur la proportionnalité. Sa transposition au Maroc exige de tenir compte de l'architecture de supervision, du cadre juridique existant, de la structure du marché et des priorités nationales. Ce chapitre propose une lecture en quatre temps : les acquis, les spécificités, les opportunités et une feuille de route.

## 5.1 Un socle institutionnel et juridique déjà structuré

Le Maroc dispose d'une supervision financière sectorielle bien établie, articulée autour de trois autorités et complétée par des institutions transversales.

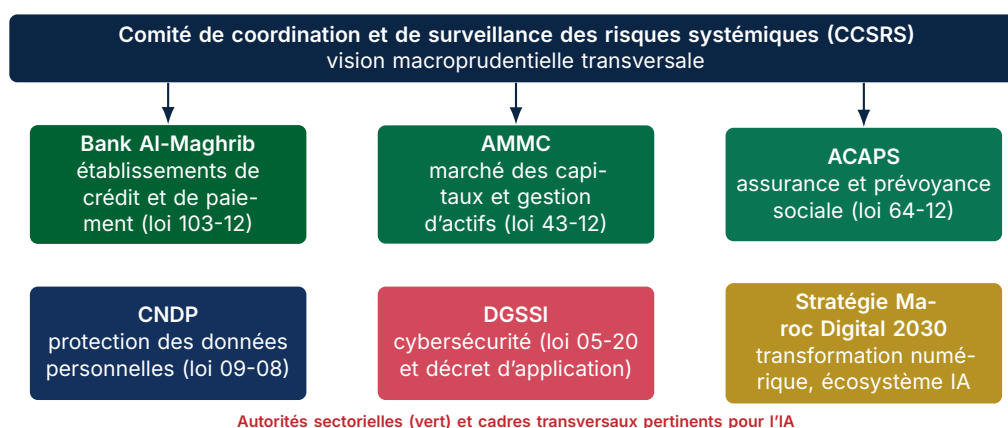


**FIG. 5.1** : Les acteurs marocains concernés par l'adoption de l'IA dans la finance

Ce dispositif offre des points d'ancrage naturels pour plusieurs pratiques du FSB. La **loi 09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, sous le contrôle de la CNDP, couvre déjà une partie des exigences de la PS7 (licéité des traitements, transferts transfrontaliers, droits des personnes). La **loi 05-20** relative à la cybersécurité et son décret d'application donnent un cadre aux exigences de la PS11 pour les entités et infrastructures d'importance vitale. Les dispositifs prudentiels de Bank Al-Maghrib en matière de contrôle interne, de gestion des risques opérationnels, de continuité d'activité et d'externalisation constituent la base sur laquelle intégrer les PS2, PS3 et PS12. Enfin, l'expérience acquise par Bank Al-Maghrib avec sa directive de 2021 sur la gestion des risques financiers liés au climat montre la capacité du superviseur à intégrer un risque émergent dans le cadre de gouvernance des banques, ce qui constitue un précédent méthodologique utile pour l'IA.

## 5.2 Les spécificités qui conditionnent la transposition

| Exigence du FSB                      | Point d'appui marocain                                                                   | Écart à combler                                                                           |
|--------------------------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Gouvernance (PS1-PS3)</b>         | Cadres de gouvernance, de contrôle interne et de risque opérationnel des trois autorités | Absence, à notre connaissance, de lignes directrices prudentielles spécifiques à l'IA     |
| <b>Données (PS7)</b>                 | Loi 09-08, contrôle de la CNDP                                                           | Qualité des données d'entraînement, lignage, données synthétiques et non conventionnelles |
| <b>Explicabilité et client (PS8)</b> | Règles de protection de la clientèle et de traitement des réclamations                   | Droit à explication et à contestation des décisions automatisées en matière de crédit     |
| <b>Cyber (PS11)</b>                  | Loi 05-20, DGSSI, dispositifs de continuité                                              | Scénarios d'attaques fondées sur l'IA, identité des agents, hypertrucages et KYC          |
| <b>Tiers (PS12)</b>                  | Règles d'externalisation existantes                                                      | Concentration envers des fournisseurs étrangers de nuage et de modèles de fondation       |
| <b>Adaptabilité (PS4)</b>            | Programmes de formation, coopération avec les universités                                | Cadre public-privé dédié à l'IA (consortium, bac à sable)                                 |

**Tab. 5.1** : Correspondance entre les exigences du FSB et le cadre marocain

### 5.2.1 Un secteur bancaire concentré et projeté en Afrique

Le paysage bancaire marocain se caractérise par un nombre restreint de grands groupes, dont plusieurs ont une présence significative en Afrique subsaharienne. Cette configuration a deux conséquences. D'une part, la **proportionnalité** du FSB se traduit concrètement : les grands groupes, à profil systémique et transfrontalier, relèvent du niveau d'exigence le plus élevé, tandis que les établissements de paiement, les sociétés de financement ou les petits acteurs du financement collaboratif (loi 15-18) peuvent appliquer une version adaptée. D'autre part, le risque de **comportements homogènes** identifié par le FSB prend une dimension particulière : si quelques groupes adoptent les mêmes modèles de fondation ou les mêmes solutions de notation, les décisions de crédit et de couverture pourraient se corréliser, au Maroc comme dans les filiales africaines. La coordination entre Bank Al-Maghrib et les superviseurs des pays d'accueil devient alors un enjeu de supervision consolidée de l'IA.

### 5.2.2 Une dépendance technologique externe

Comme la plupart des économies émergentes, le Maroc dépend largement de fournisseurs étrangers pour l'informatique en nuage, le matériel de calcul et les modèles de fondation. La PS12 trouve ici une résonance forte : clauses de localisation des traitements, compatibilité avec les règles de transfert de la loi 09-08, plans de sortie et analyse de la concentration à l'échelle du système. Les investissements nationaux dans les centres de données et les capacités de calcul, portés par la stratégie Maroc Digital 2030, peuvent réduire cette dépendance, sans toutefois l'éliminer pour les modèles les plus avancés.

### 5.2.3 Une réalité linguistique singulière

Les interactions avec la clientèle se font en arabe, en darija, en amazighe et en français. Les modèles de langage généralistes, entraînés majoritairement sur l'anglais, présentent souvent une performance moindre et moins stable sur la darija. Les exigences du FSB en matière de performance (PS9), de biais (PS7) et de transparence client (PS8) impliquent donc des tests spécifiques par langue et par population : un agent conversationnel bancaire qui comprend mal la darija risque de traiter de manière inéquitable les clients les

moins à l'aise avec le français, c'est-à-dire souvent les publics que l'inclusion financière cherche à atteindre.

#### 5.2.4 Le capital humain

La pyramide de compétences de la PS4 suppose des profils hybrides, à la fois financiers et techniques, ainsi que des validateurs et auditeurs formés à l'IA. Le Maroc forme chaque année un nombre croissant d'ingénieurs et de diplômés en science des données, mais leur rétention face à la demande internationale reste un défi. La recommandation du FSB de préserver le jugement humain et d'éviter la déqualification est particulièrement pertinente dans un marché où les compétences spécialisées sont rares.

### 5.3 Des opportunités alignées sur les priorités nationales

#### ★ Cinq cas d'usage à fort potentiel pour le Maroc

- 1. Inclusion financière et crédit aux TPE-PME.** Notation fondée sur des données alternatives (flux de paiement mobile, historique de factures) pour des entreprises sans historique bancaire, dans le prolongement de la stratégie nationale d'inclusion financière. L'étude de cas du FSB sur la détection précoce des difficultés des PME est directement transposable.
- 2. LBC/FT et lutte contre la fraude.** Consolidation des acquis du Maroc depuis sa sortie de la liste grise du GAFI en 2023, par la détection d'anomalies et la réduction des faux positifs, avec une vigilance accrue face aux hypertrucages lors de l'entrée en relation à distance.
- 3. Paiement mobile et monnaie électronique.** Analyse comportementale en temps réel pour sécuriser la croissance des portefeuilles électroniques.
- 4. Risques climatiques.** Modèles d'apprentissage automatique pour évaluer l'exposition des portefeuilles aux risques physiques (sécheresse, inondations, séismes) et de transition, en appui aux exigences de Bank Al-Maghrib sur le risque climatique et à l'assurance des événements catastrophiques. Ces modèles, souvent peu explicables, relèvent précisément des contrôles compensatoires de la PS8.
- 5. Technologie de supervision (suptech).** Exploitation des remontées réglementaires par les autorités elles-mêmes, pour détecter plus tôt les vulnérabilités.

### 5.4 Grille d'appréciation de la maturité

Le graphique suivant propose une appréciation qualitative, par l'auteur, du degré de préparation du système financier marocain sur huit dimensions dérivées des pratiques du FSB, notées de 1 (embryonnaire) à 5 (avancé). Il ne s'agit pas d'une évaluation officielle mais d'un support de discussion, destiné à hiérarchiser les chantiers.

La lecture de cette grille fait ressortir deux points forts relatifs, la protection des données et la cybersécurité, qui bénéficient de cadres législatifs dédiés, et trois chantiers prioritaires : la gouvernance prudentielle propre à l'IA, l'explicabilité au service du client et la coopération public-privé autour de l'IA.

### 5.5 Transposition des douze pratiques : propositions

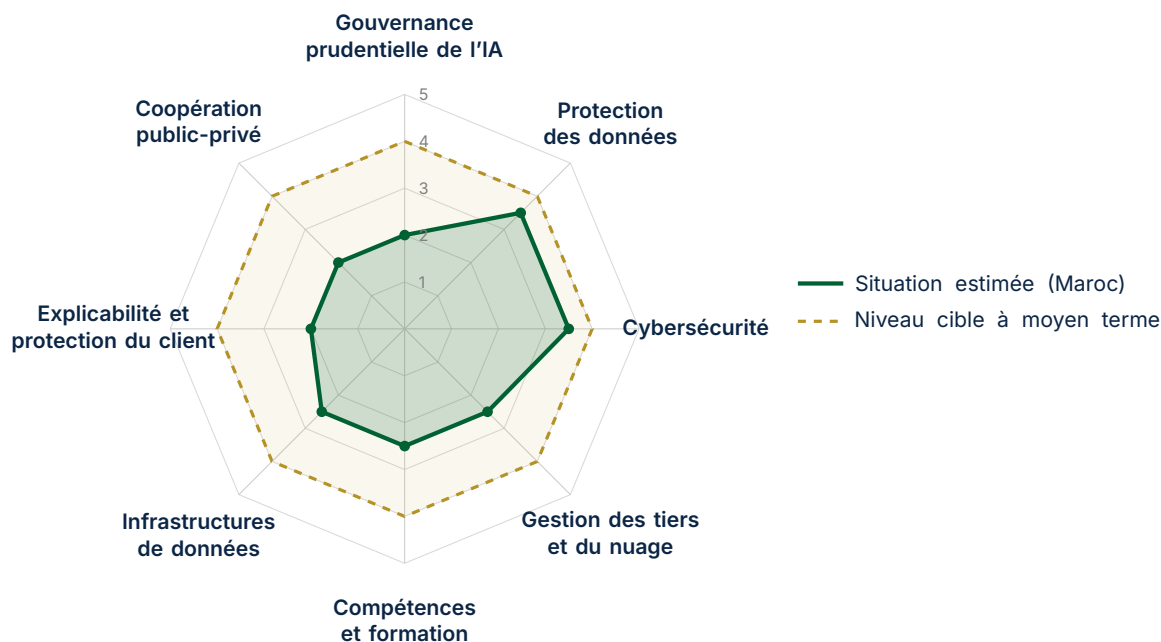


**Fig. 5.2** : Maturité du système financier marocain face aux pratiques du FSB (appréciation qualitative de l'auteur)

**Tab. 5.2** : Pistes de transposition des pratiques du FSB au Maroc

| Pratique                 | Acteurs                                   | Proposition                                                                                                                          |
|--------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>PS1 Stratégie</b>     | Conseils d'administration, autorités      | Inscrire l'IA dans les déclarations d'appétence au risque ; former les administrateurs, y compris indépendants.                      |
| <b>PS2 Gouvernance</b>   | Établissements                            | Désigner un responsable par cas d'usage matériel ; créer un comité IA dans les groupes systémiques.                                  |
| <b>PS3 Documentation</b> | Établissements, BAM, AMMC, ACAPS          | Tenir un inventaire de l'IA ; envisager une remontée périodique simplifiée aux autorités.                                            |
| <b>PS4 Adaptabilité</b>  | Autorités, universités, GPBM              | Créer un consortium national sur l'IA financière ; programmes conjoints avec les universités (Tanger, Rabat, Casablanca, Benguerir). |
| <b>PS5 Matérialité</b>   | Établissements                            | Grille commune de classement des cas d'usage, inspirée de la matrice matérialité-risque.                                             |
| <b>PS6 Sélection</b>     | Établissements                            | Privilégier des modèles explicables pour le crédit aux particuliers et aux TPE.                                                      |
| <b>PS7 Données</b>       | Établissements, CNDP                      | Lignes directrices conjointes sur l'usage de données personnelles pour l'entraînement et la RAG.                                     |
| <b>PS8 Explicabilité</b> | BAM, ACAPS, associations de consommateurs | Information du client sur l'usage de l'IA dans les décisions de crédit et de sinistres ; droit à une revue humaine.                  |

| Pratique                | Acteurs                    | Proposition                                                                                                       |
|-------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>PS9 Performance</b>  | Établissements             | Tests de performance et de biais par langue (arabe, darija, amazighe, français) et par région.                    |
| <b>PS10 Supervision</b> | Établissements             | Interdire l'autonomie totale des agents sur les opérations financières tant que les tests ne sont pas concluants. |
| <b>PS11 Cyber</b>       | DGSSI, BAM, établissements | Intégrer des scénarios d'attaques par IA et d'hypertrucages dans les exercices de crise sectoriels.               |
| <b>PS12 Tiers</b>       | Autorités, GPBM            | Clauses types communes pour les contrats d'IA ; cartographie de la concentration à l'échelle du système.          |

## 5.6 Feuille de route en trois horizons

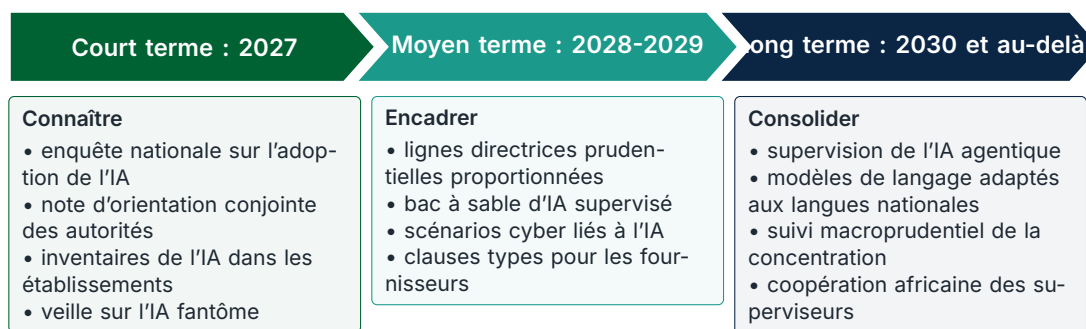


**FIG. 5.3** : Feuille de route proposée pour l'adoption responsable de l'IA au Maroc

### Trois risques à ne pas sous-estimer au Maroc

**Le risque de non-adoption.** Le FSB le souligne : rester à l'écart de l'IA expose à une perte de compétitivité et à une moindre capacité de détection de la fraude. Une réglementation trop lourde ou trop précoce pourrait creuser l'écart avec les acteurs étrangers. **Le risque d'exclusion algorithmique.** Des modèles entraînés sur des populations bancarisées et urbaines peuvent pénaliser les clients ruraux ou du secteur informel, à rebours des objectifs d'inclusion. **Le risque de dépendance.** La concentration des fournisseurs de nuage et de modèles hors du territoire pose des questions de souveraineté, de continuité et de conformité au droit des données.

## Conclusion : de la prudence à la maîtrise

Le rapport final du FSB marque une étape dans la manière dont la communauté financière internationale aborde l'intelligence artificielle. Après avoir mesuré les vulnérabilités en 2024, le FSB propose en 2026 un vocabulaire commun et une méthode. Son principal mérite est d'avoir évité deux écueils : l'enthousiasme technologique, qui ignore les risques de modèle, de concentration et d'autonomie, et la prudence paralysante, qui oublie que ne pas adopter l'IA est aussi un risque.

Trois enseignements se dégagent de cette lecture. Le premier tient à l'**ancrage dans l'existant**. Le FSB ne réclame pas une gouvernance de l'IA séparée : il demande d'adapter les cadres de risque de modèle, de résilience opérationnelle, de cybersécurité et de gestion des tiers. Cette approche limite le coût de mise en conformité et favorise la cohérence. Le deuxième tient à la **proportionnalité**, qui traverse l'ensemble des pratiques et que la matrice matérialité-risque rend opérationnelle. Le troisième tient au **basculement agentique** : en passant de la prédiction à l'action, l'IA impose d'emprunter à la sécurité informatique ses notions d'identité, de moindre privilège et de confiance zéro, et de compléter la supervision humaine par des contrôles déterministes inscrits dans le code.

Le rapport laisse toutefois plusieurs questions ouvertes. Les pratiques relatives aux systèmes multi-agents restent, de l'aveu même du FSB, naissantes. La question de la responsabilité juridique lorsqu'un agent fourni par un tiers commet une erreur n'est pas tranchée. Les indicateurs permettant de mesurer la valeur créée par l'IA font défaut. Enfin, la dimension macroprudentielle, c'est-à-dire la corrélation des comportements induite par des modèles communs, est identifiée mais peu outillée au niveau de l'établissement, qui ne peut à lui seul la maîtriser.

### ★ Pour le Maroc : une fenêtre d'opportunité

Le Maroc aborde cette transition avec des atouts : des autorités de supervision expérimentées, des cadres législatifs sur les données et la cybersécurité, une stratégie numérique nationale et un secteur bancaire capable d'investir. La publication du rapport du FSB offre l'occasion d'adopter une démarche anticipatrice, en trois temps : connaître l'état réel de l'adoption, encadrer de manière proportionnée, puis consolider la supervision de l'IA agentique et la souveraineté technologique. Le succès dépendra de la capacité à concilier innovation, inclusion financière et stabilité, et à faire de l'IA un levier au service des objectifs nationaux, notamment l'inclusion des TPE et la gestion des risques climatiques.

Pour la recherche en économie et en gestion, ce rapport ouvre un programme de travail fécond : mesurer empiriquement l'adoption de l'IA dans les établissements des économies émergentes, évaluer son effet sur la qualité du crédit et l'inclusion, tester les biais des modèles selon les langues et les territoires, et étudier les canaux par lesquels l'homogénéité des modèles pourrait affecter la stabilité financière. L'intelligence artificielle n'est ni une menace à contenir ni une solution miracle : elle est une technologie dont la valeur dépend, en dernier ressort, de la qualité de la gouvernance qui l'encadre.

# Annexes

## Annexe A. Les douze pratiques saines du FSB

|      |                                                                                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PS1  | <b>Orientation stratégique et supervision.</b> Le conseil d'administration et la direction générale alignent l'adoption et la gouvernance de l'IA sur le modèle d'affaires, l'appétence au risque et la stratégie de l'institution.                                              |
| PS2  | <b>Gouvernance et responsabilité.</b> Les institutions définissent des rôles et responsabilités clairs et maintiennent un cadre de gouvernance approprié pour une adoption responsable de l'IA.                                                                                  |
| PS3  | <b>Cadre de gestion des risques et documentation.</b> Les institutions adoptent des cadres de gestion des risques qui traitent efficacement les risques de l'IA et comprennent des processus de documentation de l'usage de l'IA et d'évaluation de la matérialité et du risque. |
| PS4  | <b>Adaptabilité organisationnelle.</b> Les institutions apprennent, s'adaptent et ajustent leur supervision, leur gouvernance, leurs pratiques de gestion des risques et leurs capacités à mesure que l'IA évolue.                                                               |
| PS5  | <b>Matérialité et risque.</b> Les institutions mettent en œuvre une approche efficace et systématique d'évaluation de la matérialité et du risque des cas d'usage dès la conception et par la suite.                                                                             |
| PS6  | <b>Processus de sélection.</b> Lors de la sélection des modèles ou systèmes d'IA, les institutions prennent en compte les objectifs d'affaires, les besoins opérationnels et techniques, ainsi que la matérialité et les risques des cas d'usage.                                |
| PS7  | <b>Gouvernance des données.</b> Les institutions établissent une gouvernance des données appropriée afin de disposer de données adaptées à l'entraînement, aux tests et à l'utilisation de l'IA (exactes, complètes, cohérentes, fiables, sécurisées).                           |
| PS8  | <b>Explicabilité et transparence.</b> Les institutions comprennent les différences d'explicabilité entre types d'IA, adoptent si possible une IA plus explicable ou des contrôles compensatoires, et assurent une transparence adaptée aux parties prenantes.                    |
| PS9  | <b>Gestion de la performance.</b> Les institutions évaluent la performance des cas d'usage à proportion de leur matérialité et de leur risque, par des évaluations, des tests et un suivi continu.                                                                               |
| PS10 | <b>Supervision humaine.</b> Les institutions mettent en œuvre une supervision humaine appropriée et effective, selon la matérialité, le risque, l'autonomie, la complexité et l'explicabilité des cas d'usage.                                                                   |
| PS11 | <b>Risques cyber et TIC.</b> Les institutions gèrent les risques cyber et TIC liés à l'IA, notamment par des scénarios dédiés dans les tests et exercices, le partage d'information et l'utilisation d'outils d'IA.                                                              |

**PS12**

**Risques liés aux tiers.** Les institutions gèrent les risques liés à leurs dépendances envers des tiers en matière d'IA : performance, transparence, qualité des données, chaîne d'approvisionnement, concentration et continuité d'activité.

## Annexe B. Glossaire bilingue

| Terme français                               | Terme anglais                         | Définition résumée                                                                                                                          |
|----------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IA agentique</b>                          | <i>Agentic AI</i>                     | Systèmes autonomes capables de décider, d'apprendre de leurs interactions et de poursuivre des objectifs sans intervention humaine directe. |
| <b>IA générative</b>                         | <i>Generative AI</i>                  | IA qui produit des contenus nouveaux (texte, image, vidéo), généralement à partir de modèles de fondation.                                  |
| <b>IA fantôme</b>                            | <i>Shadow AI</i>                      | Outils d'IA adoptés par des employés sans autorisation ou pour des usages non approuvés.                                                    |
| <b>IA embarquée</b>                          | <i>Embedded AI</i>                    | IA intégrée dans des services tiers qui ne sont pas présentés comme des services d'IA.                                                      |
| <b>Dérive des données</b>                    | <i>Data drift</i>                     | Situation où les données utilisées ne correspondent plus aux circonstances actuelles.                                                       |
| <b>Dérive du modèle</b>                      | <i>Model drift</i>                    | Modification des relations entre les entrées et les sorties d'un modèle.                                                                    |
| <b>Explicabilité</b>                         | <i>Explainability</i>                 | Mesure dans laquelle un humain comprend comment un modèle produit ses sorties ; c'est un continuum.                                         |
| <b>Génération augmentée par récupération</b> | <i>Retrieval-Augmented Generation</i> | Technique qui améliore la précision d'un modèle de langage en puisant dans un corpus sélectionné.                                           |
| <b>Humain dans la boucle</b>                 | <i>Human-in-the-loop</i>              | Approbation humaine de toutes les décisions prises par l'IA.                                                                                |
| <b>Matérialité</b>                           | <i>Materiality</i>                    | Importance d'un cas d'usage pour la viabilité, les opérations critiques et la conformité de l'institution.                                  |
| <b>Modèle à poids ouverts</b>                | <i>Open-weight model</i>              | Modèle dont les poids sont publics, sans que les autres composantes le soient nécessairement.                                               |
| <b>Modèle de fondation</b>                   | <i>Foundation model</i>               | Modèle entraîné sur des données larges et adaptable à de nombreuses tâches.                                                                 |
| <b>Moindre agence</b>                        | <i>Least agency</i>                   | Octroi à un agent des seules permissions nécessaires à son objectif.                                                                        |

| Terme français                   | Terme anglais                 | Définition résumée                                                                      |
|----------------------------------|-------------------------------|-----------------------------------------------------------------------------------------|
| <b>Résilience opérationnelle</b> | <i>Operational resilience</i> | Capacité à assurer les opérations critiques malgré les perturbations.                   |
| <b>Risque de modèle</b>          | <i>Model risk</i>             | Conséquences défavorables de décisions fondées sur des modèles erronés ou mal utilisés. |
| <b>Équipe rouge</b>              | <i>Red teaming</i>            | Effort structuré de test visant à trouver les failles d'un système d'IA.                |

## Références

- Financial Stability Board (2026), *Sound Practices for Responsible Adoption of Artificial Intelligence (AI)*, rapport final, 15 octobre.
- Financial Stability Board (2026), *Sound Practices for financial institutions' responsible AI adoption : Overview of consultation responses*, octobre.
- Financial Stability Board (2025), *Monitoring AI Adoption and Related Vulnerabilities in the Financial Sector*, octobre.
- Financial Stability Board (2024), *The Financial Stability Implications of Artificial Intelligence*, novembre.
- Financial Stability Board (2023), *Enhancing Third-party Risk Management and Oversight : A Toolkit for Financial Institutions and Financial Authorities*, décembre.
- Financial Stability Board (2017), *Artificial intelligence and machine learning in financial services*, novembre.
- Basel Committee on Banking Supervision (2021), *Principles for operational resilience*; (2025), *Principles for the sound management of third-party risk*.
- IOSCO (2026), *Supervisory Toolkit for AI Use in Capital Markets*, rapport final, mai.
- IAIS (2025), *Application Paper on the supervision of artificial intelligence*, juillet.
- NIST (2023), *AI Risk Management Framework (AI RMF 1.0)*; NIST (2025), *Adversarial Machine Learning : A Taxonomy and Terminology of Attacks and Mitigations*.
- ISO/IEC 42001 :2023, *Information technology, Artificial intelligence, Management system*.
- The MindForge Consortium (2026), *AI Risk Management : Operationalisation Handbook*.
- Royaume du Maroc, loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (2009).
- Royaume du Maroc, loi n° 05-20 relative à la cybersécurité (2020).
- Royaume du Maroc, loi n° 103-12 relative aux établissements de crédit et organismes assimilés; loi n° 43-12 relative à l'AMMC; loi n° 64-12 portant création de l'ACAPS; loi n° 15-18 relative au financement collaboratif.
- Ministère de la Transition numérique et de la Réforme de l'administration, *Maroc Digital 2030*.