RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANKING EUROPÉEN & MARCHÉS FINANCIERS

Nous avons une politique, une norme et un certificat — que prouvent-ils ?

Un Board Briefing Report sur l'architecture de gouvernance de l'IA — EU AI Act, ISO/IEC 42001, NIST AI RMF, tests et preuves.

Reza Monshizadeh · Monshizadeh.com · 7 min de lecture

01 SITUATION

Chacun est présenté comme le cadre. Aucun ne répond à la même question.

SUPPOSONS LA SITUATION SUIVANTE

La direction présente au conseil :

- une politique d'IA alignée sur l'EU AI Act,
- un programme de certification ISO/IEC 42001,
- une méthodologie de risque fondée sur le NIST AI Risk Management Framework,
- et un processus de tests techniques.

> Un certificat ne remplace pas une matrice de correspondance réglementaire.

> Une évaluation des risques ne démontre pas qu'un contrôle fonctionne.

> Un résultat de test ne prouve pas que les bonnes obligations juridiques ont été identifiées.

LA QUESTION AU CONSEIL

La direction peut-elle démontrer comment les obligations juridiques, la gouvernance organisationnelle, les décisions de risque et les tests des systèmes s'articulent dans un modèle opérationnel unique et traçable ?

02 MANAGEMENT SUMMARY

Trois points d’orientation pour le conseil.

01

Un cadre complet comporte quatre couches reliées

Le droit définit les obligations. Le système de management rend la gouvernance reproductible. La méthode de risque structure le jugement. Les tests et les preuves montrent comment systèmes et contrôles fonctionnent. Complémentaires — non interchangeables.

02

Un certificat n’est pas une matrice de correspondance

ISO/IEC 42001 peut fournir un système de management de l’IA certifiable — elle n’établit pas automatiquement la conformité à l’EU AI Act. **EN 18286** a été élaborée spécifiquement pour l’exigence de management de la qualité de l’AI Act.

03

Un Framework Stack, pas une simple étiquette

La preuve requise est une ligne traçable reliant l’obligation au contrôle, au test, au responsable et à la preuve conservée — une architecture gouvernée couvrant l’ensemble du périmètre IA et de son cycle de vie.

Une institution peut acheter un certificat. Elle ne peut pas acheter la matrice de correspondance.

03 CALIBRATION DE LA QUALITÉ DE RÉPONSE

Le statut RAG calibre la qualité de la réponse. Il ne juge pas l'institution.

DIMENSION	VERT	AMBRE	ROUGE
Inventaire	Un périmètre IA unique, gouverné et réconcilié	Un inventaire existe, mais certaines IA tierces ou intégrées restent hors périmètre	*« Nous savons où se trouve notre IA. »*
Cartographie juridique	Matrice de correspondance entre exigences et contrôles par cas d'usage	Une cartographie juridique existe mais n'est pas reliée aux contrôles	*« Nous sommes alignés sur l'EU AI Act. »*
Périmètre de certification	Le périmètre, les exclusions et les frontières organisationnelles sont explicites	Un certificat existe, mais son périmètre n'est pas réconcilié avec l'inventaire IA	*« Nous préparons une certification ISO. »*
Méthode de risque	La classification détermine le parcours de gouvernance	Des scores de risque existent, mais ne modifient ni les exigences ni les approbations	*« Nous appliquons le cadre NIST. »*
Tests	Les seuils d'acceptation sont liés à l'usage prévu	Des tests sont réalisés, mais séparés du cas d'usage ou de la décision	*« Le fournisseur a testé le modèle. »*
Responsabilité	Un responsable nommé détient l'autorité d'approuver, d'arrêter et de faire remonter	Des comités interviennent, mais l'autorité personnelle reste floue	*« Cela passe par le comité IA. »*
Tiers	Les preuves, les obligations de notification des changements et les droits d'audit sont définis	Des clauses contractuelles existent, mais les preuves opérationnelles sont incomplètes	*« C'est la responsabilité du fournisseur. »*
Information au conseil	L'efficacité, les exceptions et les décisions sont rapportées	L'état d'avancement est présenté, mais l'efficacité des contrôles n'est pas visible	*« Le programme est dans les temps. »*

VERT n'est pas un certificat. VERT est une ligne traçable de l'obligation à la preuve.

04 LE FRAMEWORK STACK

Quatre couches. Quatre questions différentes. Un modèle opérationnel.

01 CADRE JURIDIQUE

Que doit faire l'institution ?

EU AI Act, RGPD, DORA, réglementation financière et exigences applicables en matière de produits, d'emploi et de protection des consommateurs.

CE QUE CETTE COUCHE NE PROUVE PAS À ELLE SEULE

Que l'institution a traduit les obligations en contrôles opérationnels.

02 SYSTÈME DE MANAGEMENT

Qui gouverne l'IA, au moyen de quelles responsabilités et de quels processus ?

ISO/IEC 42001, ISO/IEC 38507 et, pour l'exigence de management de la qualité de l'AI Act, EN 18286.

CE QUE CETTE COUCHE NE PROUVE PAS À ELLE SEULE

Que chaque système d'IA est correctement classé, juridiquement conforme ou techniquement digne de confiance.

03 MÉTHODE DE RISQUE

Comment les risques liés à l'IA sont-ils identifiés, évalués, acceptés et traités ?

NIST AI RMF, ISO/IEC 23894, méthodologies de risque de modèle et processus de classification des risques d'entreprise.

CE QUE CETTE COUCHE NE PROUVE PAS À ELLE SEULE

Que les contrôles retenus fonctionnent efficacement.

04 TESTS & PREUVES

Qu'est-ce qui démontre que le système et ses contrôles fonctionnent comme annoncé ?

AI Verify, analyses d'impact, validation, tests de robustesse et de sécurité, tests des contrôles et vérification indépendante.

CE QUE CETTE COUCHE NE PROUVE PAS À ELLE SEULE

Que chaque obligation applicable a été identifiée et attribuée.

Chaque couche répond à une question différente. Aucune ne répond à la suivante.

05 QUI DOIT RÉPONDRE

Une réponse de gestion intégrée — conduite par le dirigeant responsable de l'IA d'entreprise, de la technologie ou des données, conjointement avec le dirigeant responsable des risques ou de la conformité.

CONTRIBUTEURS REQUIS

■ Responsabilité métier	■ Juridique	■ Conformité	■ Risques
■ Risque de modèle	■ Technologie	■ Données	■ Cybersécurité
■ Protection des données	■ Risque tiers	■ Achats	■ Audit interne

NOTE DE RESPONSABILITÉ

L'appartenance à un comité n'est pas équivalente à une responsabilité personnelle. Le responsable nommé doit détenir l'autorité nécessaire pour approuver, restreindre, suspendre ou faire remonter l'usage de l'IA concerné.

AUDIT INTERNE

L'audit interne peut évaluer la conception et l'efficacité opérationnelle. Il ne doit pas devenir propriétaire de la gouvernance de première ligne de l'IA.

06 PREUVES QUE LE CONSEIL DOIT DEMANDER

Dix artefacts qui rendent l'architecture vérifiable.

01 **Inventaire IA de l'entreprise**
Un périmètre gouverné couvrant les IA développées en interne, achetées, intégrées et fournies par des tiers.

02 **Carte d'architecture des cadres**
La relation entre le droit, les systèmes de management, les méthodes de risque, les tests et la vérification indépendante.

03 **Matrice de correspondance réglementaire**
Les exigences applicables reliées aux politiques, contrôles, responsables, tests et preuves.

04 **Responsabilités et droits de décision**
Pouvoirs d'approbation, d'acceptation du risque résiduel, d'intervention, de suspension et d'escalade.

05 **Méthodologie de classification**
Classification juridique, matérialité, impact client, criticité opérationnelle et réversibilité.

06 **Carte des contrôles du cycle de vie**
Les exigences depuis l'initiation et l'achat jusqu'au déploiement, au changement et au retrait.

07 **Analyse d'impact et des risques**
Une analyse achevée pour un cas d'usage à conséquences significatives.

08 **Dossier de test et de validation**
Objectifs de test, méthodes, seuils d'acceptation, exceptions et approbation.

09 **Déclaration du périmètre de certification**
Entités, processus, systèmes, exclusions et frontières de certification couverts.

10 **Dossier d'information au conseil**
Exposition au risque, exceptions, incidents, changements significatifs, actions en retard et décisions requises.

Un cas d'usage doit pouvoir être suivi de la classification juridique à l'état de production actuel — **sans modification des périmètres, des définitions ou des responsables entre les documents.**

07 GOVERNANCE CHECK

SIGNAUX D'ALERTE

Ces réponses peuvent sembler rassurantes en réunion de conseil. Elles ne sont pas encore décisionnelles.

- ⚠ *« Nous appliquons le cadre NIST. »*
- ⚠ *« Nous sommes alignés sur l'EU AI Act. »*
- ⚠ *« Nous préparons une certification ISO. »*
- ⚠ *« Le fournisseur a testé le modèle. »*
- ⚠ *« Une personne approuve le résultat. »*
- ⚠ *« C'est couvert par la politique IA. »*
- ⚠ *« Ce n'est qu'un outil interne. »*
- ⚠ *« Le cadre est en cours de déploiement. »*

Aucune de ces affirmations n'est nécessairement erronée. **Elles ne constituent simplement pas une preuve suffisante pour que le conseil puisse s'y fier.**

08 PATH TO GREEN

Six conditions pour une architecture gouvernée.

01 Architecture nommée
Les quatre couches sont définies et utilisées de manière cohérente.

02 Matrice de correspondance construite
Les obligations sont reliées aux contrôles, responsables, tests et preuves.

03 La classification détermine le parcours
La matérialité et le statut juridique déterminent l'intensité de la gouvernance.

04 Norme de preuve définie
Les dossiers requis sont précisés avant l'autorisation de mise en production.

05 Tiers inclus
Les modèles, données, outils et infrastructures externes restent dans le périmètre de gouvernance.

06 Efficacité surveillée
L'information au conseil montre le fonctionnement des contrôles, les exceptions et les décisions — pas uniquement l'avancement du programme.

QUESTION SUIVANTE POUR LE CONSEIL

Prenez un système d'IA susceptible d'affecter de manière significative un client, un salarié, une transaction ou un processus critique — la direction peut-elle montrer, dans une seule chaîne de preuves, le droit applicable, le responsable désigné disposant de l'autorité requise, la décision de risque approuvée, les contrôles opérationnels, les résultats des tests, le mécanisme d'intervention humaine, les dépendances à des tiers et l'état de production actuel ?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Une institution peut acheter un certificat. Elle ne peut pas acheter la matrice de correspondance.

Le conseil ne doit pas demander quel cadre l'institution applique. Il doit demander si un usage de l'IA à conséquences significatives peut être retracé de l'obligation jusqu'à la preuve opérationnelle.

SOURCES SÉLECTIONNÉES

Regulation (EU) 2024/1689 — Artificial Intelligence Act.

Regulation (EU) 2026/1744 — Digital Omnibus on AI.

CEN-CENELEC — EN 18286: Quality Management for EU AI Act Purposes.

ISO/IEC 42001:2023 — AI Management Systems.

ISO/IEC 42006:2025 — Certification of AI Management Systems.

NIST — AI Risk Management Framework & Generative AI Profile.

AI Verify Foundation — Testing Framework.

EBA — AI Act Implications for Banking and Payments.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com