RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANKING EUROPEO & MERCATI FINANZIARI

Abbiamo una policy, uno standard e un certificato — che cosa dimostrano?

Un Board Briefing Report sull'architettura di governance dell'IA — EU AI Act, ISO/IEC 42001, NIST AI RMF, test ed evidenze.

Reza Monshizadeh · Monshizadeh.com · 7 min di lettura

01 SITUATION

Ciascuno viene descritto come il quadro. Nessuno risponde alla stessa domanda.

ASSUMIAMO LA SEGUENTE SITUAZIONE

Il management presenta al consiglio:

- una policy sull'IA allineata all'EU AI Act,
- un programma di certificazione ISO/IEC 42001,
- una metodologia di rischio basata sul NIST AI Risk Management Framework,
- e un processo di test tecnici.

> Un certificato non sostituisce una matrice di corrispondenza normativa.

> Una valutazione del rischio non dimostra che un controllo funzioni.

> Un risultato di test non prova che siano stati identificati gli obblighi giuridici corretti.

LA DOMANDA AL CONSIGLIO

Il management può dimostrare come obblighi giuridici, governance organizzativa, decisioni di rischio e test dei sistemi si colleghino in un unico modello operativo tracciabile?

02 MANAGEMENT SUMMARY

Tre punti di orientamento per il consiglio.

01

Un framework completo ha quattro livelli collegati

Il diritto definisce gli obblighi. Il sistema di gestione rende la governance ripetibile. La metodologia di rischio struttura il giudizio. Test ed evidenze mostrano come operano sistemi e controlli. Complementari — non intercambiabili.

02

Un certificato non è una matrice di corrispondenza

ISO/IEC 42001 può fornire un sistema di gestione dell'IA certificabile — non dimostra automaticamente la conformità all'EU AI Act. **EN 18286** è stato sviluppato specificamente per il requisito di gestione della qualità dell'AI Act.

03

Un Framework Stack, non una singola etichetta

La prova richiesta è una linea tracciabile dall'obbligo al controllo, al test, al responsabile e all'evidenza conservata — un'unica architettura governata che copra l'intera popolazione IA e il ciclo di vita.

Un'istituzione può acquistare un certificato. Non può acquistare la matrice di corrispondenza.

03 CALIBRAZIONE DELLA QUALITÀ DELLA RISPOSTA

Lo stato RAG calibra la qualità della risposta. Non giudica l'istituzione.

DIMENSIONE	VERDE	AMBRA	ROSSO
Inventario	Un'unica popolazione IA governata e riconciliata	Esiste un inventario, ma alcune IA di terzi o integrate restano fuori dal perimetro	*"Sappiamo dove si trova la nostra IA."*
Mappatura giuridica	Matrice di corrispondenza tra requisiti e controlli per caso d'uso	Esiste una mappa giuridica, ma non è collegata ai controlli	*"Siamo allineati all'EU AI Act."*
Perimetro di certificazione	Perimetro, esclusioni e confini organizzativi sono espliciti	Esiste un certificato, ma il suo perimetro non è riconciliato con l'inventario IA	*"Siamo in fase di certificazione ISO."*
Metodologia di rischio	La classificazione determina il percorso di governance	Esistono punteggi di rischio, ma non modificano requisiti o approvazioni	*"Applichiamo il quadro NIST."*
Test	Le soglie di accettazione sono collegate all'uso previsto	I test vengono eseguiti ma sono scollegati dal caso d'uso o dalla decisione	*"Il fornitore ha testato il modello."*
Responsabilità	Un responsabile nominato ha l'autorità di approvare, fermare ed effettuare escalation	I comitati sono coinvolti, ma l'autorità personale non è chiara	*"Passa attraverso il comitato IA."*
Terze parti	Evidenze, obblighi di notifica delle modifiche e diritti di verifica sono definiti	Esistono clausole contrattuali, ma le evidenze operative sono incomplete	*"È responsabilità del fornitore."*
Informativa al consiglio	Efficacia, eccezioni e decisioni vengono riportate	Viene presentato lo stato di avanzamento, ma l'efficacia dei controlli non è visibile	*"Il programma è in linea con il piano."*

VERDE non è un certificato. VERDE è una linea tracciabile dall'obbligo all'evidenza.

04 IL FRAMEWORK STACK

Quattro livelli. Quattro domande diverse. Un modello operativo.

01 QUADRO GIURIDICO

Che cosa deve fare l'istituzione?

EU AI Act, GDPR, DORA, regolamentazione finanziaria e requisiti applicabili in materia di prodotti, lavoro e tutela dei consumatori.

CHE COSA NON DIMOSTRA DA SOLO
Che l'istituzione abbia tradotto gli obblighi in controlli operativi.

02 SISTEMA DI GESTIONE

Chi governa l'IA e attraverso quali responsabilità e processi?

ISO/IEC 42001, ISO/IEC 38507 e, per il requisito di gestione della qualità dell'AI Act, EN 18286.

CHE COSA NON DIMOSTRA DA SOLO
Che ogni sistema di IA sia correttamente classificato, conforme alla legge o tecnicamente affidabile.

03 METODOLOGIA DI RISCHIO

Come vengono identificati, valutati, accettati e trattati i rischi dell'IA?

NIST AI RMF, ISO/IEC 23894, metodologie di rischio di modello e processi aziendali di classificazione del rischio.

CHE COSA NON DIMOSTRA DA SOLO
Che i controlli selezionati operino efficacemente.

04 TEST & EVIDENZE

Che cosa dimostra che il sistema e i suoi controlli funzionano come dichiarato?

AI Verify, valutazioni d'impatto, validazione, test di robustezza e sicurezza, test dei controlli e verifica indipendente.

CHE COSA NON DIMOSTRA DA SOLO
Che ogni obbligo applicabile sia stato identificato e assegnato.

Ogni livello risponde a una domanda diversa. Nessuno risponde a quella successiva.

05 CHI DOVREBBE RISPONDERE

Una risposta integrata del management — guidata dal dirigente responsabile dell'IA a livello aziendale, della tecnologia o dei dati, insieme al dirigente responsabile dei rischi o della compliance.

CONTRIBUTORI RICHIESTI

■ Responsabilità di business	■ Legale	■ Compliance	■ Rischi
■ Rischio di modello	■ Tecnologia	■ Dati	■ Cybersecurity
■ Protezione dei dati	■ Rischio terze parti	■ Approvvigionamenti	■ Revisione interna

NOTA SULLA RESPONSABILITÀ

L'appartenenza a un comitato non equivale alla responsabilità personale. Il responsabile nominato deve detenere l'autorità necessaria per approvare, limitare, sospendere o effettuare escalation sull'uso dell'IA interessato.

REVISIONE INTERNA

La Revisione interna può valutare la progettazione e l'efficacia operativa. Non dovrebbe diventare proprietaria della governance IA di prima linea.

06 EVIDENZE CHE IL CONSIGLIO DOVREBBE RICHIEDERE

Dieci artefatti che rendono verificabile l’architettura.

01 **Inventario IA aziendale**
Un’unica popolazione governata che copra IA sviluppate internamente, acquistate, integrate e fornite da terzi.

02 **Mappa dell’architettura dei quadri di riferimento**
La relazione tra diritto, sistemi di gestione, metodologie di rischio, test e verifica indipendente.

03 **Matrice di corrispondenza normativa**
Requisiti applicabili collegati a policy, controlli, responsabili, test ed evidenze.

04 **Responsabilità e diritti decisionali**
Autorità di approvazione, accettazione del rischio residuo, intervento, sospensione ed escalation.

05 **Metodologia di classificazione**
Classificazione giuridica, materialità, impatto sul cliente, criticità operativa e reversibilità.

06 **Mappa dei controlli del ciclo di vita**
Requisiti dall’avvio e dall’approvvigionamento fino a implementazione, modifica e dismissione.

07 **Valutazione d’impatto e del rischio**
Una valutazione completata per un caso d’uso ad alto impatto.

08 **Registro di test e validazione**
Obiettivi, metodi, soglie di accettazione, eccezioni e approvazione.

09 **Dichiarazione del perimetro di certificazione**
Entità, processi, sistemi, esclusioni e confini di certificazione coperti.

10 **Pacchetto informativo per il consiglio**
Esposizione al rischio, eccezioni, incidenti, modifiche rilevanti, azioni scadute e decisioni richieste.

Un caso d’uso dovrebbe essere tracciabile dalla classificazione giuridica allo stato attuale in produzione — **senza cambiare popolazioni, definizioni o responsabili tra i documenti.**

07 GOVERNANCE CHECK

SEGNALI DI ALLERTA

Queste risposte possono sembrare rassicuranti in una riunione del consiglio. Non sono ancora adeguate a sostenere una decisione del consiglio.

- ⚠ *“Applichiamo il quadro NIST.”*
- ⚠ *“Una persona approva il risultato.”*
- ⚠ *“Siamo allineati all’EU AI Act.”*
- ⚠ *“È coperto dalla policy sull’IA.”*
- ⚠ *“Siamo in fase di certificazione ISO.”*
- ⚠ *“È solo uno strumento interno.”*
- ⚠ *“Il fornitore ha testato il modello.”*
- ⚠ *“Il quadro è in fase di attuazione.”*

Nessuna di queste affermazioni è necessariamente errata. **Semplicemente, non costituisce evidenza sufficiente per una decisione affidabile del consiglio.**

08 PATH TO GREEN

Sei condizioni per un’unica architettura governata.

01 Architettura definita

I quattro livelli sono definiti e utilizzati in modo coerente.

02 Matrice di corrispondenza costruita

Gli obblighi sono collegati a controlli, responsabili, test ed evidenze.

03 La classificazione determina il percorso

Materialità e status giuridico determinano l’intensità della governance.

04 Standard di evidenza definito

La documentazione richiesta è specificata prima dell’approvazione in produzione.

05 Terze parti incluse

Modelli, dati, strumenti e infrastrutture esterne restano nel perimetro di governance.

06 Efficacia monitorata

L’informativa mostra il funzionamento dei controlli, le eccezioni e le decisioni — non solo il completamento del programma.

DOMANDA SUCCESSIVA PER IL CONSIGLIO

Prendete un sistema di IA che possa incidere in modo rilevante su un cliente, un dipendente, una transazione o un processo critico — il management può mostrare, in un’unica catena di evidenze, il diritto applicabile, il responsabile designato con la necessaria autorità decisionale, la decisione di rischio approvata, i controlli operativi, i risultati dei test, il percorso di intervento umano, le dipendenze da terze parti e lo stato attuale in produzione?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Un’istituzione può acquistare un certificato. Non può acquistare la matrice di corrispondenza.

Il consiglio non dovrebbe chiedere quale quadro applica l’istituzione. Dovrebbe chiedere se un uso dell’IA ad alto impatto possa essere tracciato dall’obbligo fino all’evidenza operativa.

FONTI SELEZIONATE

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