

AI OVERSIGHT E BOARD ACCOUNTABILITY.

EVIDENZA PRIMA DELL'ASSURANCE.
RESPONSABILITÀ PRIMA DELL'INTENZIONE.

Non si tratta più solo dello strumento. **Si tratta della catena dell’evidenza.**

- 

SCENARIO

Strumenti supportati dall’AI assistono processi regolamentati — riassumono informazioni, preparano viste di rischio, supportano valutazioni di controllo o redigono motivazioni decisionali.
- 

EVENTO SCATENANTE

Alcune settimane dopo, l’output viene messo in discussione da un cliente, un auditor o un supervisor.
- 

LA DOMANDA DEL BOARD

Possiamo dimostrare, per questo output, Oversight, Ownership e Human Review in modo tracciabile?



Non si tratta solo di capire se lo strumento abbia commesso un errore.

Si tratta di capire se possiamo dimostrare **la nostra governance.**



L'UTILIZZO DELL'AI NON È PIÙ MARGINALE

Più dell'85% delle grandi banche sotto supervisione europea utilizza già l'AI in qualche forma. La domanda non è più se un'istituzione utilizzi l'AI — ma se tale utilizzo possa essere governato, controllato e dimostrato.



L'EVIDENZA PRIMA DEL DETTAGLIO DEL MODELLO

Il board non deve conoscere ogni specifica del modello. Ha però bisogno di evidenza che i material AI use cases siano chiaramente responsabilizzati, rivisti e controllati — e che tale evidenza possa essere prodotta su richiesta.



LA QUALITÀ DELLA RISPOSTA CONTA

Una risposta forte è concreta, aggiornata e documentata. Una risposta debole resta ancorata a dichiarazioni di policy, stato di progetto o responsabilità del provider.

03

CALIBRAZIONE DELLA QUALITÀ DELLA RISPOSTA

Status dell’evidenza, non valutazione dell’istituzione.

	GREEN Decisionale	AMBER Parzialmente dimostrato	RED Non decisionale
	Esiste un inventario aggiornato degli AI use cases.	L’inventario esiste, ma è incompleto.	<i>“We have an AI policy.”</i>
	Un owner chiaro è nominato per ogni use case.	L’Ownership resta a livello di progetto.	<i>“This sits with IT.”</i>
	L’Oversight è definito e documentato.	L’Oversight è descritto, ma non documentato.	<i>“The provider is responsible.”</i>
	L’AI Literacy è documentata per ruolo.	La formazione è generica, non specifica per ruolo.	<i>“Training has been completed.”</i>
	Exceptions e overrides sono monitorati.	Il monitoring esiste, ma il reporting è frammentato.	<i>“No incident has happened so far.”</i>
	Il reporting mostra rischio, valore ed evidenze di controllo.	Il board riceve status, ma non evidenza decisionale.	<i>“It is only a copilot.”</i>

GREEN is not a policy status. GREEN is an evidence status.

04

CHI DEVE RISPONDERE

Technology può possedere la piattaforma. **Il Business possiede l’impatto decisionale.**

	CIO / CTO	Architettura della piattaforma, flussi di dati e controllo tecnico. Possiede l’ambiente di deployment.
	Business Owner	Impatto decisionale, effetto sui processi e validazione dell’output. Possiede il use case e le sue conseguenze.
	CRO / Compliance / Legal	Rischio, obblighi regolamentari e protezione dei dati. Valuta la rilevanza regolamentare del comportamento del modello.
	CISO / Third-Party Risk	Sicurezza, dipendenze da provider e resilienza operativa. Gestisce i rischi legati a dipendenze esterne e tecnologia di terze parti.
	Internal Audit	Revisione indipendente della catena dell’evidenza. Conferma se i controlli esistono e se la documentazione regge a un esame.

05

EVIDENZE CHE IL BOARD DOVREBBE RICHIEDERE

Dieci artefatti che rendono una risposta verificabile.

- 01

**AI Use-Case Inventory**
Dove l’AI viene utilizzata — funzioni, processi, stato di deployment.
- 02

**Risk Classification**
Quali use cases sono materiali e richiedono oversight rafforzato.
- 03

**Ownership Map**
Chi è responsabile — per nome e funzione, non solo a livello tecnico.
- 04

**Data Classification**
Quali dati possono essere utilizzati o trattati dall’AI — uso autorizzato e origine dei dati.
- 05

**Human Oversight Design**
Dove interviene il giudizio umano — gates, review, override.

- 06

**AI Literacy Evidence**
Competenza specifica per ruolo, non solo certificati di partecipazione.
- 07

**Exception & Override Log**
Se i problemi sono visibili — overrides, escalation, incidents.
- 08

**Third-Party Dependency Map**
Dipendenze da provider, rischio di concentrazione, capacità di exit.
- 09

**Board Reporting Dashboard**
Ciò che il board riceve — tempestivo, strutturato e sufficiente.
- 10

**Decision Rights / Lifecycle Log**
Chi può scalare, limitare, riaddestrare o fermare un use case.

Segnali di allerta sulla qualità della risposta.

	<i>“We have an AI policy.”</i>	Una policy definisce un’intenzione. Non dimostra che sia implementata, monitorata o applicata a livello di use case.
	<i>“This is managed by IT.”</i>	Technology possiede la piattaforma. Il Business possiede l’impatto decisionale. Una responsabilità concentrata in una sola funzione non è sufficiente.
	<i>“The provider is responsible.”</i>	Obblighi contrattuali possono trovarsi presso il provider. L’accountability per l’output resta presso l’istituzione.
	<i>“It is only a copilot.”</i>	Se l’output influenza una decisione regolamentata, l’etichetta non riduce il requisito. Il framing non è un controllo.
	<i>“No incident has happened so far.”</i>	L’assenza di incidenti documentati non è una prova di controllo. Può anche indicare che il monitoring non funziona in modo sufficiente.
	<i>“The tool is only used internally.”</i>	Un utilizzo interno può comunque influenzare processi regolamentati, dati dei clienti o decisioni di controllo.
	<i>“We have no high-risk AI use cases.”</i>	La classificazione non sostituisce né governance, né Ownership, né evidenza.
	<i>“Training has been completed.”</i>	Le prove di partecipazione dimostrano la presenza. Non dimostrano un giudizio calibrato in un ruolo concreto.

Nessuna di queste affermazioni è necessariamente falsa. Semplicemente, non costituiscono evidenza sufficiente per una board-level reliance.

07

SEI CONDIZIONI PER UNA RISPOSTA DECISIONALE

Una risposta decisionale deve coprire questi sei ambiti.



Accountability

Ownership chiaro per decisioni e risultati.



Oversight

La Human Review è progettata e documentata.



Trasparenza

Utilizzo, limiti e canali di comunicazione sono comprensibili.



Disciplina dei dati

Finalità, qualità, accesso e protezione sono definiti.



Monitoring

Performance, drift, exceptions e risultati sono monitorati.



Evidenza

Le evidenze sono disponibili, aggiornate e verificabili.

DOMANDA SUCCESSIVA PER IL BOARD

Quale AI use case creerebbe domani il maggiore problema di accountability se un cliente, un auditor o un supervisor chiedesse una spiegazione?



**L'assurance non sostituisce l'evidenza.
L'intenzione non sostituisce l'oversight dimostrabile.**

Il board deve poter comprendere ciò che l'istituzione decide — e come tale decisione viene presa, documentata e verificata.

La Board Accountability inizia quando le risposte non suonano soltanto plausibili, ma diventano dimostrabili.