NTT DATA

Dal controllo al governo dell'AI: verso un Risk Management etico e sostenibile

Indice

1. Executive Summary

Immaginate un mondo in cui anche una piccola impresa manifatturiera possa accedere agli stessi strumenti predittivi di gestione del rischio utilizzati dalle multinazionali. Un mondo dove l'Intelligenza Artificiale non solo prevede i problemi prima che si manifestino, ma li trasforma in opportunità di crescita. Questa non è fantascienza: è la rivoluzione che sta già trasformando il Risk Management.

In un'epoca segnata da crisi globali, tensioni geopolitiche e innovazioni sempre più rapide, la gestione del rischio non può più essere relegata a funzione difensiva. Deve diventare un **motore strategico** capace di anticipare il futuro. L'Intelligenza Artificiale è il catalizzatore di questa trasformazione, così come Internet ha rivoluzionato l'accesso all'informazione e lo smartphone ha ridefinito la comunicazione.

Questo **position paper** racconta una storia di **democratizzazione e responsabilità.** Per decenni, solo le grandi corporation potevano permettersi sistemi sofisticati di Risk Management. Oggi, grazie all'AI e alle soluzioni *"as a service"*, queste capacità diventano accessibili a imprese di ogni dimensione, ridefinendo le regole della competitività. Il contesto italiano lo dimostra: secondo l'ISTAT e il Politecnico di Milano, solo l'8,2% delle imprese ha adottato almeno una tecnologia di AI, ma cresce la consapevolezza che l'intelligenza artificiale possa diventare un **fattore di fiducia e di sostenibilità**[9,10]**.**

Il documento ripercorre l'evoluzione del Risk Management, dalle sue origini probabilistiche alla rivoluzione digitale, e propone una visione concreta basata su cinque principi: un approccio proattivo che anticipa invece di reagire; l'AI come acceleratore che automatizza il complesso per liberare l'umano; una cultura del rischio diffusa in tutta l'organizzazione; una governance integrata che supera i silos organizzativi e le sue modalità di lavoro isolata di gestire i rischi; e una visione strategica che trasforma il Risk Management da costo a **leva di valore sostenibile.**

Particolare attenzione è dedicata alle **sfide etiche e regolatorie.** Non tutto ciò che è tecnicamente possibile è eticamente desiderabile. Per questo NTT DATA ha sviluppato **H2RAI – Human to Responsible AI**, la metodologia che guida le imprese verso una goverance dell'AI etica, trasparente e verificabile, e l'**Osservatorio Normativo AI**, che aiuta a trasformare l'incertezza legislativa in rischio gestibile.

Le prospettive sono chiare: entro il 2035, il Risk Management basato su AI sarà la norma, non l'eccezione. Le organizzazioni che iniziano oggi questo percorso potranno non solo proteggere il proprio business, ma anche **trasformare l'incertezza in vantaggio competitivo.**

Il messaggio finale è semplice ma essenziale: il **Risk Manager del futuro** non sarà sostituito dall'AI, ma potenziato da essa. Delegherà alle macchine l'elaborazione dei dati e si concentrerà su ciò che solo l'intelligenza umana può offrire: **creatività, giudizio etico e visione strategica.** In questo equilibrio tra uomo e macchina si gioca il futuro della governance intelligente — e la chiave per un vantaggio competitivo realmente sostenibile.

Percorsi di lettura consigliati

Tre prospettive, una stessa visione

Questo *position paper* racconta come l'Intelligenza Artificiale stia trasformando il **Risk Management** da funzione di difesa a **motore di fiducia e innovazione**. Lungo le pagine si intrecciano tre prospettive complementari — **strategica, tecnologica e culturale** — che riflettono i ruoli chiave della governance del futuro: **CEO, CIO e CRO.** Insieme, delineano una visione condivisa di impresa fondata su **responsabilità, trasparenza e valore sostenibile.**

Per i CEO – La fiducia come valore strategico

La gestione del rischio diventa leva di crescita e di sostenibilità. Per il CEO, questo documento mostra come la **fiducia sia il nuovo capitale competitivo**, nato dalla trasparenza dei processi e dall'etica dell'innovazione. La metodologia **H2RAI** propone una governance integrata in cui etica e tecnologia convergono in un vantaggio competitivo reale.

Focus consigliati:

- **Capitolo 3** → *Il Risk Management nell'era della complessità*
- **Capitolo 5** → *Regolamentazione del Risk Management: verso la governance intelligente*
- **Capitolo 7** → *Conclusioni e prospettive al 2035*

Per i CIO – L'architettura della fiducia digitale

Il CIO trova qui la chiave per comprendere come l'AI ridefinisca il perimetro del controllo e della responsabilità tecnologica. La governance del futuro non è solo un'infrastruttura, ma un **ecosistema di fiducia by design.** Il CIO diventa **architetto della trasparenza**, garante di innovazioni tracciabili, spiegabili e coerenti con i valori aziendali.

Focus consigliati:

- **Capitolo 5.3** → *Dalle regole statiche alle architetture adattive*
- **Capitolo 6** → *Il nostro approccio ERM-AI e gli acceleratori (focus su H2RAI*
- **Capitolo 7** → *Conclusioni: il ruolo del CIO nella governance del futuro*

Per i CRO, Risk e Compliance Officer – L'etica come metodo

Questo paper mostra come la tecnologia possa **amplificare, non sostituire, il giudizio umano**. Il CRO trova in **H2RAI** una risposta concreta alle nuove sfide di governance introdotte da AI Act, DORA e compliance dinamica. La supervisione umana resta il perno del controllo: la macchina elabora, ma **solo l'uomo decide.**

Focus consigliati:

- **Capitolo 3.2–3.4** → *Cultura del rischio, approccio proattivo e ciclo del rischio*
- **Capitolo 4** → *Il Risk Management e le tecnologie AI nel contesto italiano*
- **Capitolo 5.4** → *Risk, Audit e Compliance nell'era dell'AI*
- **Capitolo 6.3** → *H2RAI – Human to Responsible AI*

Per tutti – La cultura della fiducia

Oltre i ruoli, questo documento parla a chiunque creda che la tecnologia debba essere **governata, non subita**. Ogni organizzazione può fare del Risk Management una competenza collettiva. L'AI, se progettata in modo responsabile, diventa la chiave per **democratizzare la gestione del rischio** e costruire un'economia più resiliente e trasparente.

2. Premessa e obiettivi

Negli ultimi anni, le imprese si sono trovate a operare in un contesto dominato da discontinuità: crisi sanitarie, tensioni geopolitiche, shock energetici, nuove normative ESG e, soprattutto, l'irruzione dell'Intelligenza Artificiale come fattore di trasformazione sistemica. Questi eventi hanno ridefinito il concetto stesso di rischio, rendendo evidente che la gestione dell'incertezza è ormai una competenza strategica, non più un presidio tecnico o difensivo. Il Risk Management, in questa nuova prospettiva, non è un costo ma un moltiplicatore di valore: consente alle organizzazioni di anticipare i cambiamenti, prevenire le crisi e sfruttare le opportunità che emergono dai contesti instabili. **Come mostrano le più recenti analisi europee, la maturità nella gestione del rischio è oggi uno dei principali indicatori di resilienza organizzativa e di capacità di innovazione[8],[13].**

L'Intelligenza Artificiale rappresenta un punto di svolta in questo scenario. Le sue capacità predittive e analitiche rendono possibile un salto di qualità nel modo in cui le aziende individuano, valutano e mitigano i rischi: dalla reazione all'anticipazione, dal controllo puntuale alla comprensione sistemica. Allo stesso tempo, l'AI introduce nuovi rischi — etici, tecnologici e regolatori — che richiedono un approccio consapevole e integrato.

2.1. Obiettivi del documento

Questo documento nasce con l'intento di mostrare come il **Risk Management** stia evolvendo in un mondo segnato da complessità e discontinuità, e come l'**Intelligenza Artificiale** ne stia diventando un fattore di trasformazione decisivo. L'obiettivo principale è aiutare le organizzazioni a comprendere che la gestione del rischio non è più una funzione di controllo, ma una **leva strategica** per creare valore, orientare le decisioni e sostenere la crescita.

Il *paper* vuole chiarire cosa significhi oggi fare Risk Management, illustrandone i principi fondamentali e le sue applicazioni in un contesto in cui la tecnologia consente un accesso più ampio a strumenti analitici avanzati. L'AI, in particolare, sta **democratizzando la gestione del rischio,** permettendo anche a realtà medio-piccole di adottare modelli predittivi e di migliorare la propria capacità di anticipazione.

Infine, il documento presenta l'approccio metodologico di **NTT DATA**, fondato su una visione proattiva e sistemica del rischio e sull'integrazione tra innovazione tecnologica e responsabilità etica. L'obiettivo è mostrare come sia possibile trasformare l'incertezza in un **motore di crescita sostenibile**, in cui l'Intelligenza Artificiale amplifica — senza sostituirla — la capacità umana di analisi, giudizio e visione.

2.2. La nostra expertise applicata al Risk Management

La storia di NTT DATA è una storia di evoluzione tecnologica e di responsabilità. Dalle origini nel settore delle telecomunicazioni giapponesi fino alla posizione attuale tra i principali player globali della consulenza e dei servizi IT, l'azienda ha sempre interpretato l'innovazione come leva per creare valore sostenibile.

Questa visione guida anche il nostro impegno nel Risk Management, dove uniamo competenze tecnologiche, metodologiche e strategiche per supportare imprese e istituzioni nella costruzione di soluzioni di gestione del rischio evoluti e scalabili. Le nostre esperienze spaziano dallo sviluppo di framework di *Enterprise Risk Management* all'implementazione di soluzioni GRC integrate e di piattaforme di **AI applicata alla previsione, alla compliance e alla cybersecurity**.

L'approccio di NTT DATA si fonda su un principio chiave: la tecnologia deve essere progettata "**by design**" per integrare la gestione del rischio sin dalle prime fasi dei processi di innovazione. In questo modo, aiutiamo le organizzazioni a passare da una visione difensiva del rischio a una **cultura dell'anticipazione**, in cui l'incertezza diventa un fattore di crescita e di apprendimento collettivo[4]

2.3. Il Ruolo del Risk Management: dall'intuizione alla scienza dell'anticipazione

Il Risk Management nasce da qualcosa di profondamente umano: la necessità di **anticipare l'incertezza**. Ogni giorno, senza accorgercene, gestiamo il rischio. Decidiamo se prendere l'ombrello, valutiamo l'ora in cui partire per evitare il traffico, scegliamo un investimento o stipuliamo un'assicurazione. Sono gesti ordinari, ma dietro di essi si nasconde la stessa logica che guida le imprese quando cercano di prevedere un evento imprevisto o mitigare una perdita potenziale: **identificare, valutare, decidere.**

Nel corso dei secoli, questa intuizione si è trasformata in scienza. Dalle riflessioni di Pascal e Fermat sulla probabilità nel Seicento, alle prime polizze marittime dell'epoca mercantile, fino ai modelli di *Enterprise Risk Management* sviluppati nel Novecento, l'uomo ha progressivamente imparato a tradurre la paura in metodo, la casualità in analisi. Ogni crisi — dalle turbolenze finanziarie del 2008 alla pandemia, dalle interruzioni globali delle supply chain fino alle tensioni geopolitiche più recenti — ha spinto le organizzazioni a fare un passo avanti, costringendole a **prevedere meglio e reagire prima.**

Oggi, nell'era digitale, questo percorso compie una nuova evoluzione: il Risk Management non è più una funzione di difesa, ma un **motore di anticipazione strategica.** Non si limita a calcolare probabilità o impatti, ma esplora le connessioni tra eventi, individua segnali deboli, valuta scenari e costruisce modelli di resilienza. In un'azienda manifatturiera può significare sensori che segnalano anomalie prima di un fermo macchina; in un ospedale, algoritmi che prevedono i picchi di accesso ai pronto soccorso; nel settore energetico, sistemi che stimano in anticipo la vulnerabilità di una rete rispetto a eventi climatici estremi.

In tutte queste situazioni, il principio è lo stesso: **trasformare il rischio da minaccia a linguaggio decisionale.** Il rischio non scompare, ma diventa leggibile, misurabile e, soprattutto, gestibile. La sua forza non è più nella paura, ma nella conoscenza. Per questo il Risk Manager moderno non è più un controllore o un revisore, ma un **interprete della complessità.** È la figura che traduce i dati in scenari, le informazioni in scelte, l'incertezza in strategia. La sua missione non è eliminare il rischio, ma **governarlo** e trarne valore.

Oggi, gli standard internazionali come l'**ISO 31000** e le linee guida europee (EBA, EIOPA, ESMA) insistono sulla necessità

di un approccio olistico e integrato: la gestione del rischio non è più una procedura, ma una cultura. Una cultura che insegna alle organizzazioni a convivere con la complessità, a leggerla e, quando possibile, ad anticiparla[7].

2.4. L'Intelligenza Artificiale come motore di innovazione nel Risk Management

Immaginare il futuro del Risk Management significa, in un certo senso, pensare a **Minority Report**. Non per evocare un mondo di controllo onnisciente, ma per cogliere l'idea di una tecnologia capace di **vedere prima per agire meglio.** Quella che nella finzione era una distopia fondata sul *"pre-crimine",* nel mondo reale diventa un'occasione concreta: usare i dati per **anticipare i rischi prima che si manifestino**, con strumenti che rendono l'incertezza più gestibile e la decisione più consapevole.

L'**Intelligenza Artificiale** rappresenta oggi il principale motore di questa trasformazione. Grazie alla capacità di elaborare enormi volumi di dati in tempo reale, l'AI permette di individuare schemi ricorrenti, correlazioni inattese e segnali deboli che sfuggono alla percezione umana. È così che nascono i nuovi modelli predittivi: algoritmi che apprendono dai comportamenti passati per stimare probabilità future, offrendo alle organizzazioni un vantaggio competitivo fondato sulla **conoscenza anticipata.**

Questa logica trova un parallelo, interessante ma delicato, nel fenomeno del **predictive policing**, ovvero l'uso dell'AI per stimare dove o quando potrebbero verificarsi eventi criminali[15]. Sebbene in ambito sociale queste pratiche abbiano sollevato critiche legate a bias e discriminazioni, nel mondo aziendale lo stesso principio può essere reinterpretato in chiave etica e produttiva: **prevedere non per controllare, ma per proteggere**. Invece di anticipare crimini, si anticipano frodi, guasti, interruzioni operative, minacce cyber o non conformità regolamentari. Il Risk Management diventa così una forma di "prevenzione costruttiva", che coniuga potenza tecnologica e responsabilità umana.

Oggi i casi d'uso concreti sono numerosi: sistemi bancari che rilevano transazioni sospette in pochi millisecondi, piattaforme industriali che prevedono guasti alle macchine con settimane d'anticipo, catene di fornitura globali che identificano in tempo reale vulnerabilità logistiche o geopolitiche[9],[11]. La differenza non è solo nella velocità di analisi, ma nella profondità dello sguardo: non si tratta più di reagire a un evento, ma di **progettare la resilienza.**

La vera rivoluzione, tuttavia, sta nella **democratizzazione dell'intelligenza predittiva.** Grazie al cloud computing e ai modelli *as a service*, anche le piccole e medie imprese possono accedere a capacità analitiche avanzate che un tempo erano prerogativa esclusiva delle grandi organizzazioni. Questo cambiamento abbassa le barriere di costo e competenza, aprendo la strada a una gestione del rischio **più diffusa, inclusiva e sistemica.**

Ma l'intelligenza artificiale non è priva di rischi propri. L'affidamento crescente ai modelli predittivi introduce nuove vulnerabilità: distorsioni nei dati, mancanza di trasparenza, automatismi che rischiano di sostituire il giudizio umano. Per questo il futuro del Risk Management richiede una **governance etica e verificabile**, capace di integrare la potenza computazionale con la supervisione dell'esperienza e del discernimento umano.

L'obiettivo non è creare sistemi infallibili, ma costruire organizzazioni **capaci di apprendere dal rischio.** L'AI non sostituirà l'uomo: lo **amplificherà**, liberandolo dalla complessità operativa per restituirgli il compito più alto: immaginare, valutare, decidere. Nel punto di incontro tra la freddezza dell'algoritmo e la sensibilità del giudizio umano nasce il nuovo Risk Management: una disciplina che non si limita a difendere dal futuro, ma che contribuisce a **progettarlo con responsabilità.**

3. Risk Management nell'era della complessità

Il rischio non è più solo la misura di ciò che la prima legge di Murphy recita, ma è la **misura di quanto siamo disposti a cambiare** ed in questo senso il Risk Management non è una funzione aziendale ma un **modo di pensare il futuro.**

Il Risk Management moderno nasce da questa consapevolezza: non serve a eliminare l'incertezza — impresa impossibile — ma a **trasformarla in conoscenza utile.** La sua essenza è la capacità di leggere i segnali prima che diventino eventi, di costruire risposte prima che si manifestino le crisi. In altre parole, è una f**orma di intelligenza organizzativa** che permette alle persone e alle imprese di convivere con l'imprevedibilità, senza esserne travolte.

3.1. Le caratteristiche del Risk Management moderno

Si è già detto come il Risk Management contemporaneo sia figlio delle crisi che lo hanno preceduto e che da queste lezioni sia nata la convinzione che il rischio non sia solo qualcosa da gestire, ma una **prospettiva attraverso cui comprendere il mondo che cambia.**

Oggi il Risk Management non è più confinato a una funzione tecnica o di controllo, ma sta, seppur lentamente, progressivamente diventando **una leva strategica di resilienza e competitività.** La sua forza sta nel connettere saperi diversi — tecnologia, governance, finanza, persone — in un unico linguaggio di anticipazione. Le imprese più evolute non attendono che il rischio si manifesti: lo mappano, lo simulano, lo prevedono. E, soprattutto, lo integrano nella strategia aziendale.

Tre sono i tratti che ne definiscono la maturità:

Proattività

Le organizzazioni non si limitano a reagire agli eventi, ma costruiscono capacità di lettura e previsione. Attraverso modelli di scenario *analysis e data intelligence,* imparano a individuare i segnali deboli che preannunciano un cambiamento.

Integrazione

Il rischio non appartiene più a un singolo dipartimento: attraversa la strategia, la compliance, la sostenibilità, l'IT e le risorse umane. I modelli di *Enterprise Risk Management*, formalizzati nello standard **ISO 31000**[1] e nel **CoSO Framework**[2] hanno inesorabilmente segnato la fine dell'approccio "a silos". Oggi il Risk Management è un processo trasversale che connette strategia e governance, trasformando la gestione dell'incertezza in **vantaggio competitivo**. In una banca, ciò significa unire il rischio operativo a quello reputazionale e normativo; in una pubblica amministrazione, allineare la sicurezza informatica con la protezione dei dati; in una utility, integrare la gestione ambientale con quella industriale.

Tecnologia come fattore abilitante

La digitalizzazione ha cambiato il volto del rischio, ma anche gli strumenti per gestirlo. Le piattaforme di analisi predittiva e i sistemi di *continuous monitoring* permettono di misurare in tempo reale indicatori che un tempo richiedevano mesi di osservazione. La tecnologia, però, non sostituisce la competenza umana: la amplifica. Un algoritmo può segnalare una tendenza, ma solo un manager può attribuirle un significato. Il valore nasce dal dialogo tra i due — **la precisione della macchina e l'intuito dell'esperienza**.

In sintesi, il Risk Management moderno non è più un esercizio difensivo, ma una **forma di intelligenza collettiva**. Rende visibile ciò che è incerto, trasforma la complessità in comprensione e l'incertezza in decisione. È il ponte tra la vulnerabilità e la fiducia.

3.2. La cultura del rischio come leva proattiva

Alla base di ogni modello di Risk Management efficace non ci sono solo processi o strumenti, ma una **cultura condivisa del rischio.** La tecnologia può misurare, i modelli possono prevedere, ma solo una cultura diffusa può rendere queste capacità realmente utili e sostenibili.

La *risk culture* rappresenta la maturità con cui un'organizzazione **riconosce, discute e assume il rischio** come parte della propria identità. Non si tratta di evitare l'incertezza, ma di imparare a governarla collettivamente dal board fino ai livelli operativi. Un'impresa con una cultura del rischio sviluppata non subisce i cambiamenti, li **interpreta**; non reagisce alle crisi, le **anticipa**.

Costruire questa cultura significa promuovere trasparenza, consapevolezza e responsabilità. Significa creare spazi in cui l'errore diventa fonte di apprendimento e la segnalazione di un rischio è vista come un atto di fiducia, non come una denuncia. Il tone *from the top* — la coerenza tra i valori dichiarati e i comportamenti del management — è il punto di partenza di questa trasformazione.

Nell'era dell'Intelligenza Artificiale, la cultura del rischio assume un valore ancora più strategico in quanto l'adozione di modelli predittivi e automatizzati richiede che le persone comprendano **come e perché le macchine decidono** sapendo però mantenere la supervisione umana nei momenti critici. Senza una cultura del rischio, la tecnologia rischia di diventare miope, ma se affiancate possono invece diventare **una leva di fiducia e responsabilità condivisa**.

La **cultura del rischio** è quindi il fondamento invisibile della proattività: non una regola o una procedura, ma un **atteggiamento diffuso** che consente a ogni individuo di leggere l'incertezza, agire con consapevolezza e contribuire alla resilienza collettiva.

3.3. Le nuove sfide del Risk Management nell'era dell'AI

L'Intelligenza Artificiale ha introdotto un territorio di rischio del tutto nuovo, dove **la tecnologia e la governance coincidono**. I modelli di *machine learning* e le piattaforme predittive trasformano dati in decisioni, ma questa trasformazione solleva domande di conformità, responsabilità e trasparenza che toccano il cuore stesso della *compliance* moderna.

L'**AI Act europeo**[3] stabilisce un principio chiave: i sistemi di AI devono essere sottoposti a un **processo strutturato di gestione del rischio**, fondato su analisi preventiva, documentazione e controllo continuo. Non è solo un adempimento normativo, ma l'affermazione di una nuova forma di *governance del rischio algoritmico* a cui le organizzazioni sono chiamate a dimostrare non soltanto che un modello funziona, ma che **funziona in modo equo, sicuro e tracciabile.**

Questa prospettiva si integra con altre cornici normative già consolidate:

• il **GDPR**, che introduce la logica del *privacy by design*;

• il **DORA Regulation**[4], che impone la resilienza operativa digitale come requisito di vigilanza;

• e gli standard **ISO 31000**[1] e **CoSO ERM**[2], che richiamano l'importanza di una gestione integrata dei rischi tecnologici e di controllo interno.

Per i Chief Risk Officer e gli Audit Committee, ciò significa che la gestione dell'AI non può essere confinata al perimetro IT ma deve essere parte del **sistema di controllo interno.** Devono esistere politiche, ruoli e procedure che garantiscano la validazione dei modelli, la revisione periodica delle decisioni automatizzate e la possibilità di effettuare un *audit trail* completo.

Le autorità di vigilanza, come EBA ed EIOPA[6,7], si stanno muovendo nella stessa direzione: chiedono che il rischio digitale e quello algoritmico siano integrati nelle metodologie di controllo e che i processi decisionali basati su AI siano **tracciabili, spiegabili e proporzionati al loro impatto.** Il Risk Management, quindi, diventa anche **compliance preventiva,** un presidio che garantisce non solo la stabilità dell'impresa, ma la sua legittimità regolatoria.

3.4. Il ciclo del rischio

Il Risk Management non è una sequenza di controlli, ma un processo di apprendimento continuo. Il suo ciclo classico — identificare, valutare, mitigare, monitorare — oggi diventa circolare e predittivo, non più lineare.

Identificare significa riconoscere rischi nuovi e interconnessi: cyber, ESG, reputazionali, tecnologici. **Valutare** implica combinare dati quantitativi e giudizio esperto, andando oltre le metriche per leggere i contesti. **Mitigare** non è solo installare barriere, ma progettare cultura e processi resilienti, dalla *data governance* al *crisis management*. **Monitorare** richiede visione in tempo reale: *dashboard, KRI e continuous auditing* trasformano la misurazione in previsione.

Questo approccio è coerente con le direttive e i framework citati (**ISO 31000, CoSO ERM, ...**) aiutando il Risk Management nell'evolversi in **intelligenza collettiva**, un meccanismo che connette persone, tecnologia e governance per anticipare il futuro invece di reagire ad esso quando questo diventa il presente.

3.5. L'approccio trasversale

Il rischio non risiede in un'area, ma **attraversa l'intera impresa** e quindi il Risk Management moderno deve essere trasversale e connettivo: una **rete di competenze** che integra finanza, tecnologia, compliance e sostenibilità.

Nel **Finance**, la gestione del rischio è parte della strategia per il controllo del capitale. Nell'**IT**, le norme **DORA** e **ISO/IEC 27001** impongono governance digitale integrata. Nella **Compliance**, AI Act e GDPR ridefiniscono la responsabilità algoritmica. Nel **manifatturiero**, i rischi di supply chain vengono monitorati con AI predittiva; nell'HR, la carenza di competenze è trattata come rischio strategico; nell'**ESG**, il rischio reputazionale diventa misura di sostenibilità.

Questa convergenza rende il Risk Management la **spina dorsale della governance moderna** connotandosi come un linguaggio comune tra Risk, Audit e Compliance che unisce etica, dati e decisione.

3.6. Verso un nuovo paradigma di governance

In questo scenario, il confine tra gestione del rischio, audit e compliance si assottiglia fino quasi a scomparire. Le imprese più evolute stanno adottando un approccio **"governance by design"**, in cui la valutazione del rischio, la verifica di conformità e la responsabilità etica vengono integrate sin dalle prime fasi di sviluppo di processi e tecnologie.

Questo paradigma è già visibile nei nuovi orientamenti europei. Le linee guida EBA 2024[6] sulla *internal governance* impongono che i comitati di controllo abbiano piena visibilità sui rischi ICT e AI; l'**EIOPA Opinion 2025**[7] introduce il principio di *human oversight* come requisito permanente per l'uso di sistemi intelligenti in ambito assicurativo. In parallelo, la normativa ESG (Tassonomia UE e CSRD[5]) estende la responsabilità del Risk Management al piano della

sostenibilità e della reputazione.

Per un'organizzazione moderna, questo significa sviluppare un modello di controllo che unisca **accountability, trasparenza e auditabilità**. Il rischio non è più soltanto un tema operativo, ma il luogo in cui si misurano etica e sostenibilità della governance.

È su questo terreno che si innesta la metodologia **H2RAI – Human to Responsible AI**. Nata in NTT DATA come evoluzione delle diverse lesson learnt di progetti dove AI era una parte rilevante, H2RAI traduce i principi normativi *AI act* in un framework operativo che collega tre dimensioni:

1. Risk Management, con valutazioni ex ante e monitoraggio continuo;

2. Compliance, allineata ai requisiti dell'AI Act, GDPR e DORA;

3. Audit Responsabile, che garantisce verificabilità e tracciabilità lungo tutto il ciclo di vita dell'AI.

In questo modello, la tecnologia non è lasciata a se stessa: è **governata dall'intelligenza umana.** È la sintesi di un nuovo equilibrio tra innovazione e controllo, dove l'AI diventa parte della governance aziendale, non una variabile esterna da sorvegliare.

4. Il Risk Management e le tecnologie AI nel contesto italiano

Nel 2025, le imprese italiane operano in un ambiente caratterizzato da **rischi sempre più interconnessi e dinamici:** crisi geopolitiche, eventi climatici estremi, cyber minacce e nuove normative che cambiano con rapidità. Si è già più volte ricordato come in questo contesto la gestione del rischio non possa più essere un presidio tecnico o difensivo, ma debba diventare una **competenza strategica** per garantire la resilienza organizzativa e la competitività del sistema produttivo nazionale.

Basandoci su informazioni disponibili in letteratura, in questo capitolo analizziamo tre prospettive complementari:

• lo **stato di maturità del Risk Management** nelle imprese italiane;
• la **diffusione e le applicazioni dell'Intelligenza Artificiale**;
• la **convergenza crescente tra i due ambiti** che sta ridisegnando i modelli di governance verso forme predittive e integrate.

L'Intelligenza Artificiale, in particolare, rappresenta la discontinuità più significativa di questa fase: automatizza i processi, aumenta la capacità previsionale e riduce i tempi di reazione, ma soprattutto, sposta il Risk Management da funzione di controllo a **motore di decisione e fiducia,** rendendolo più accessibile e misurabile.

4.1. Risk Management

Negli ultimi anni, il Risk Management ha acquisito un peso crescente nelle strategie aziendali.

Nel **2024**, il

46% delle imprese italiane lo considera una leva di crescita e competitività

35% dichiara di aver adottato un sistema di Risk Management integrato

5% ne è priva o lo percepisce come attività accessoria[8]

L'andamento della percezione del rischio negli ultimi cinque anni evidenzia un'evoluzione chiara: dopo la contrazione seguita alla pandemia, il **2024** segna una ripresa significativa, indicando che le aziende stanno riscoprendo il valore strategico del rischio come fattore di resilienza[8]. Le imprese più mature hanno già compreso che il rischio non è solo un vincolo, ma una chiave di lettura del cambiamento. La **cultura del rischio** diventa così un vantaggio competitivo: le organizzazioni che investono in processi, dati e formazione mostrano maggiore stabilità e capacità di innovazione.

Tuttavia, la maturità del sistema italiano resta eterogenea. Il divario tra le grandi imprese e le PMI è ancora ampio, sia in termini di strumenti adottati che di governance interna. Proprio questo gap apre la strada a una **democratizzazione del Risk Management**, resa possibile dalle tecnologie emergenti e dai modelli di gestione basati su AI.

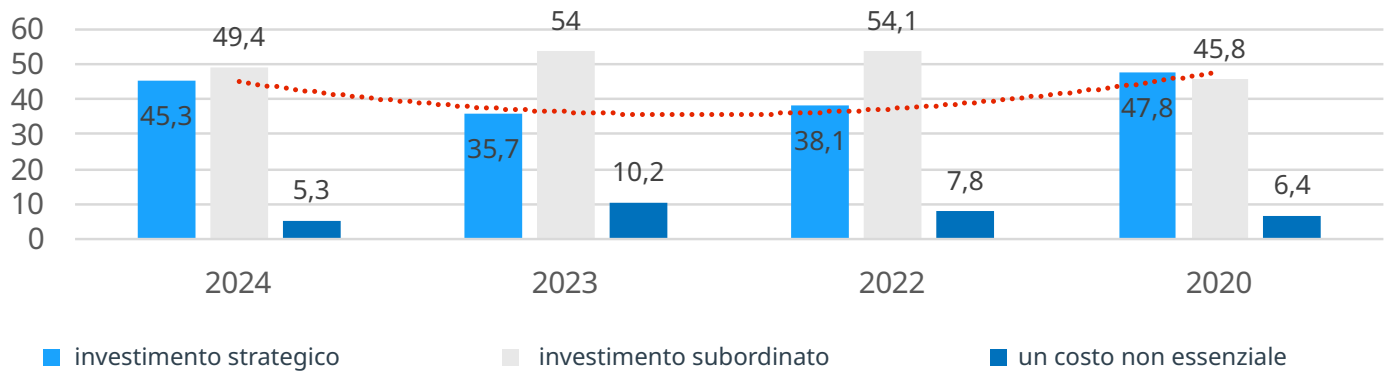


Figura 1 – Percezione dell'investimento in Risk Management (2020–2024)

Il grafico mostra come la percezione del Risk Management nelle imprese italiane stia evolvendo da funzione difensiva a leva strategica. Dopo un calo durante la fase post-pandemica (2022–2023), il 2024 segna una ripresa: il **45,3% delle aziende** considera oggi il Risk Management un investimento strategico, contro il 35,7% del 2023. Parallelamente, la quota di imprese che lo percepisce come costo non essenziale si riduce progressivamente.

Questo andamento evidenzia una **crescente maturità culturale**: le aziende stanno riconoscendo che investire nella gestione del rischio significa **investire in stabilità e competitività**. Il dato suggerisce anche un riallineamento con i trend europei, dove la cultura del rischio è sempre più integrata nei modelli di governance e sostenibilità.

La maturazione culturale si riflette anche nell'evoluzione dei modelli organizzativi, come mostra la Figura 2.

La tendenza lineare evidenziata nel grafico indica una **convergenza verso modelli integrati di governance**, in cui le funzioni di controllo dialogano tra loro e il rischio è trattato come fattore trasversale alla strategia. Questo andamento riflette anche l'influenza delle nuove normative europee e della crescente attenzione alla sostenibilità e alla resilienza operativa.

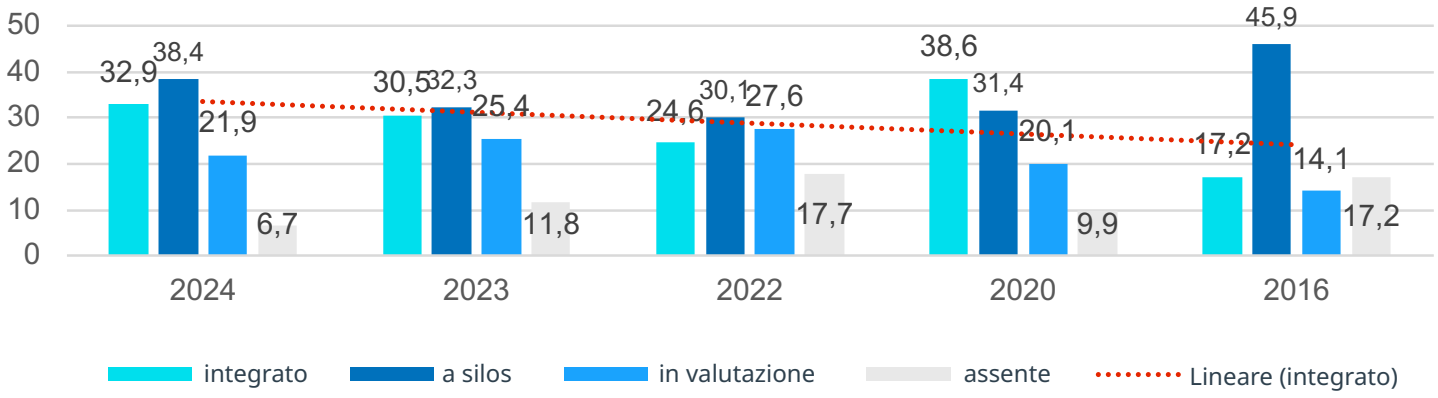


Figura 2 – Modello di Risk Management nelle imprese italiane (2016–2024)

Il grafico mostra come negli ultimi anni si osservi una **progressiva crescita dei sistemi integrati**, passati dal **17%** del 2016 al → **33%** del 2024, segno di una maturità sempre più diffusa e di un approccio meno frammentato alla gestione dei rischi. Parallelamente, diminuisce la quota di aziende che operano con modelli "a silos" o privi di una struttura formalizzata, mentre aumenta quella delle imprese "in valutazione", a conferma di un percorso di transizione ancora in atto.

4.2. L'adozione dell'Intelligenza Artificiale in Italia

L'Intelligenza Artificiale è ormai una **leva strutturale della trasformazione industriale e dei modelli di governance aziendale**. Nel 2024 il mercato italiano dell'AI ha raggiunto un valore di circa **1,2 miliardi di euro**, registrando una crescita del 58% rispetto all'anno precedente[11].

Questa espansione, confermata anche dal **CINEAS – Osservatorio di Risk Management 2024**[12], riflette un'accelerazione diffusa nei processi di digitalizzazione, ma anche la necessità di gestire i nuovi rischi generati dall'adozione di tecnologie predittive.

Secondo i dati **ISTAT**, solo l' **8,2%** delle imprese italiane con almeno 10 addetti utilizza oggi almeno una tecnologia di intelligenza artificiale[10]. Una percentuale che sale sensibilmente tra le grandi imprese, ma che resta molto bassa tra le piccole e medie: solo il **7%** delle piccole e il **15%** delle medie hanno avviato progetti di AI, valori confermati dall'**Osservatorio Artificial Intelligence 2025 del Politecnico di Milano**9. Il dato indica un **divario di maturità digitale e di cultura tecnologica** che ancora limita la diffusione dell'AI nel tessuto produttivo italiano, dominato da PMI.

Le aree di applicazione più frequenti riguardano l'**automazione dei processi, la progettazione e il monitoraggio dei prodotti**, il c**ustomer care** e la **sicurezza dei dipendenti**, con valori medi compresi tra il 15% e il 22% delle aziende che hanno già implementato soluzioni di AI in questi ambiti[9]. La tendenza è chiara: la tecnologia non è più confinata ai reparti IT, ma entra nelle funzioni di governo del rischio, dove abilita l'analisi predittiva, la classificazione delle anomalie e la gestione anticipata di eventi complessi.

Il CINEAS – Osservatorio di Risk Management 2025[13] evidenzia come l'AI stia contribuendo a ridefinire il ruolo del Risk Manager, da presidio operativo a figura strategica capace di leggere in tempo reale correlazioni e vulnerabilità sistemiche. Questo cambiamento si accompagna però a un aumento dei rischi "nuovi": bias algoritmici, opacità decisionale e affidabilità dei modelli emergono tra le principali preoccupazioni di chi utilizza l'AI in ambiti regolati.

L'Allianz Risk Barometer 2025[14] conferma che, per il 38% delle imprese italiane, i rischi legati all'AI e alla gestione dei dati sono oggi una **priorità assoluta** nella mappa dei rischi emergenti, superando persino quelli legati alle interruzioni di business o alla sicurezza informatica tradizionale. Questo dato rafforza l'esigenza di integrare l'AI nella governance del rischio con approcci metodologici che ne garantiscano **trasparenza, tracciabilità e supervisione umana**.

Nonostante la bassa percentuale di adozione, il potenziale è enorme. Le previsioni formulate dal **Politecnico di Milano**[9] stimano che, entro il 2027, oltre il 25 % delle PMI italiane avrà introdotto almeno un sistema di AI per la gestione dei processi o dei rischi operativi. La crescita sarà trainata da modelli as a service e da piattaforme di governance scalabili, che permetteranno alle imprese di accedere a tecnologie avanzate senza sostenere costi proibitivi.

In questo scenario, l'approccio proposto da **H2RAI – Human to Responsible AI** assume un ruolo abilitante. La metodologia sviluppata da NTT DATA offre alle imprese un framework per integrare l'intelligenza artificiale nella gestione del rischio in modo proporzionato e conforme al nuovo **AI Act europeo**[3].

H2RAI consente di coniugare innovazione, etica e responsabilità, assicurando che le decisioni automatizzate siano verificabili e supervisionate. È questa la condizione necessaria perché l'AI diventi, anche per il tessuto delle PMI italiane, una **tecnologia di fiducia**, capace di generare valore sostenibile e diffuso.

4.3. Risk Management e AI: considerazioni sui dati

Il 2025 segna un punto di svolta nella relazione tra **Risk Management e Innovazione Tecnologica**. Dai più recenti rapporti del **Cineas – Osservatorio di Risk Management 2025**[13] emerge con chiarezza che le imprese italiane stanno attraversando una fase di **integrazione funzionale** tra la gestione del rischio e l'introduzione di tecnologie avanzate, in particolare l'Intelligenza Artificiale. Non si tratta di un'evoluzione marginale ma di un **cambio di paradigma** che ridefinisce il modo stesso in cui le organizzazioni comprendono, misurano e affrontano l'incertezza.

Secondo il Cineas, oltre il **60 % dei Risk Manager** ritiene che l'AI diventerà, entro tre anni, lo strumento principale per l'analisi predittiva e la valutazione dei rischi complessi[13]. Parallelamente, l'**Osservatorio Artificial Intelligence 2025 del Politecnico di Milano**[10] evidenzia come l'AI sia già impiegata per correlare dati eterogenei e individuare precocemente anomalie operative o comportamentali. Questa convergenza fra competenza analitica umana e capacità di calcolo algoritmica consente di passare da un modello di **controllo reattivo** a uno di **prevenzione predittiva**, in cui il rischio viene gestito in tempo reale e il dato diventa un asset di fiducia.

Il **Cineas 2025**[13] conferma inoltre che le imprese più innovative stanno adottando **piattaforme integrate di Risk Management e AI Governance**, in grado di connettere cybersecurity, compliance, sostenibilità e business continuity e in grado di abilitare la c.d. governance adattiva, nella quale i modelli di rischio vengono aggiornati automaticamente in base ai dati che cambiano e agli eventi esterni.

Tale approccio riduce i tempi di risposta ai rischi operativi e migliora la capacità di rendicontazione verso autorità di vigilanza e stakeholder.

Ma l'innovazione non elimina la responsabilità: la compresenza di uomo e macchina introduce nuovi rischi – bias, errori di correlazione, dipendenza dai dati – che richiedono una governance solida.

L'**Allianz Risk Barometer 2025**[14] colloca infatti i **rischi legati all'uso non controllato dell'AI** tra le prime cinque minacce per le aziende europee, insieme a cyber risk e instabilità geopolitica.

Questi risultati indicano che l'innovazione, per essere sostenibile, deve essere accompagnata da **principi di etica, trasparenza e supervisione umana**.

La convergenza tra Risk Management e AI richiede quindi **metodologie integrat**e che combinino analisi predittiva, responsabilità e trasparenza, un modello ibrido in cui la tecnologia supporta il giudizio umano senza sostituirlo e in cui la gestione del rischio diventa una competenza collettiva capace di trasformare la complessità in conoscenza.

Le proiezioni al 2030 indicano che oltre il **40% delle aziende italiane di media dimensione** adotterà soluzioni di **Risk Intelligence**, basate su integrazione di dati, processi e tecnologie avanzate[13]. Il Risk Management si trasforma così in una disciplina **cognitiva e relazionale**, in cui l'uomo resta il garante del significato e la tecnologia lo strumento che ne amplifica la visione.

5. Regolamentazione del Risk Management: verso la governance intelligente

5.1. Il nuovo ruolo della regolamentazione

Per la prima volta, la regolamentazione non rincorre la tecnologia: la accompagna e la modella. Con l'Intelligenza Artificiale, il diritto e la governance si muovono sullo stesso piano evolutivo, in cui le regole non servono più solo a controllare ciò che l'uomo decide, ma anche ciò che **le macchine apprendono e suggeriscono[3].**

L'entrata in vigore dell'AI Act (UE 2024/1689)[3] segna un passaggio storico introducendo un sistema di gestione del rischio proporzionato al livello di impatto dei sistemi intelligenti. Maggiore è il potenziale effetto sull'uomo o sull'organizzazione, più stringenti devono essere i requisiti di trasparenza, sicurezza e supervisione umana. È la traduzione normativa del principio: **non esiste innovazione senza responsabilità.**

In questo scenario, le funzioni di **Risk, Audit e Compliance** non possono più operare come presìdi distinti, ma convergono in un **ecosistema integrato di fiducia.** La tecnologia diventa parte del controllo: gli algoritmi vengono addestrati non solo a eseguire decisioni, ma a rispettare valori, principi e regole di conformità.

5.2. Gli standard come base della fiducia algoritmica

Gli **standard internazionali** restano il linguaggio comune del Risk Management, ma stanno cambiando forma. Il principio del *risk-based thinking* — introdotto da **ISO 31000[1]** e consolidato dal **CoSO ERM Framework[2]** — si estende oggi al campo dell'Intelligenza Artificiale, trasformandosi in *AI-risk-based thinking*. Significa riconoscere che i sistemi intelligenti, come gli esseri umani, possono sbagliare, apprendere e migliorare, e che la gestione del rischio deve accompagnare questo ciclo evolutivo.

Nuovi riferimenti come la norma ISO/IEC 42001:2023 (AI Management System)[14] offrono un modello di controllo adattivo che collega etica, responsabilità e sicurezza. A livello europeo, l'**EBA[6]** e l'**EIOPA[7]** sottolineano la necessità di *human oversight* permanente e di audit continuo sui modelli automatizzati. La fiducia diventa così misurabile, la compliance si sposta dal piano formale a quello computazionale: ciò che conta non è solo la policy, ma la **prova digitale della sua applicazione.**

Gli standard, un tempo percepiti come vincoli, diventano strumenti di **accountability proattiva.** Consentono alle imprese di dimostrare in modo oggettivo la propria

affidabilità, anche verso stakeholder e autorità di vigilanza. In questa prospettiva, la regolamentazione si trasforma da barriera a **fattore abilitante dell'innovazione.**

5.3. Dalle regole statiche alle architetture adattive

L'AI impone di superare la logica della regola statica per abbracciare **architetture normative adattive**. Il Regolamento DORA (UE 2022/2554)[4], dedicato alla resilienza digitale, ne è un esempio: introduce il principio di *operational continuity by design*, che richiede alle organizzazioni di garantire capacità di risposta, recovery e reporting automatico in caso di incidente ICT. Lo stesso vale per la CSRD (UE 2022/2464)[5] e la **Tassonomia Europea**, che rendono obbligatorio misurare e comunicare i rischi ESG, spingendo le imprese a integrare le metriche di sostenibilità nei processi di controllo e pianificazione.

In questo nuovo ecosistema, la conformità non è più statica né episodica ma **dinamica, data-driven e predittiva** imponendo alla funzioni di controllo di evolvere in sinergia con la tecnologia. L'**Audit,** ad esempio, utilizza strumenti di analisi automatica per verificare la coerenza dei modelli di AI; la **Compliance** impiega algoritmi per intercettare in anticipo modifiche normative (*rif. par. 6.4.1* Osservatorio Normativo AI di NTT DATA); il **Risk Management** adotta piattaforme di *early warning* per identificare vulnerabilità e correlazioni non evidenti. Si passa così da un modello di vigilanza reattiva a uno di **governance adattiva** dove il controllo cresce insieme al rischio e ne condivide la velocità.

5.4. Risk, Audit e Compliance nell'era dell'AI

La **convergenza tra le tre funzioni di controllo** è ormai un fatto. Il **Risk Management** definisce il perimetro di accettabilità del rischio, l'**Audit** ne verifica la tracciabilità e la correttezza ed infine la **Compliance** assicura l'allineamento ai principi etici e normativi. Insieme, formano una **struttura integrata di governo dell'incertezza.**

Nell'era dell'AI, questo sistema deve essere più **trasparente e verificabile**. Le decisioni automatizzate devono poter essere spiegate, le fonti dei dati documentate, le logiche dei modelli comprensibili agli auditor e ai regolatori. Il concetto di *Explainable AI (c.d **XAI** - non basta che un modello "funzioni" - cioè produca output corretti-, ma è importante che sia chiaro perché produce quel risultato, come lo ha prodotto e quali fattori lo influenzano)* non è solo un requisito tecnico, ma una **nuova frontiera del controllo interno.**

Il **Risk Manager del futuro** sarà chiamato a supervisionare non solo rischi operativi o finanziari, ma anche **rischi cognitivi** — quelli derivanti dal modo in cui l'AI interpreta, collega o amplifica le informazioni. L'Audit interno non analizzerà più soltanto processi e procedure, ma anche **codice e dataset**, validando l'affidabilità algoritmica come oggi si validano i bilanci. La Compliance, infine, passerà da funzione normativa a **funzione abilitante**, capace di integrare etica e performance in un'unica visione.

Anche in questo contesto si colloca la **metodologia H2RAI – Human to Responsible AI.** Concepita da NTT DATA, H2RAI (di cui tratteremo in maniera più estensiva nel prossimo capitolo) traduce i requisiti regolatori in processi concreti, fornendo un modello operativo per la governance responsabile dell'AI. È un framework che unisce i pilastri della gestione del rischio (**ISO 31000[1], CoSO[2]**), della resilienza digitale (**DORA[4]**) e della conformità etica (**AI Act[3], GDPR, CSRD[5]**), costruendo un'unica **architettura di fiducia.**

5.5. Verso la compliance predittiva

Il passo successivo è la **compliance che anticipa,** non che insegue e quindi l'uso dell'**Intelligenza Artificiale** nelle funzioni di controllo apre la strada alla **compliance predittiva**, un modello in cui l'AI analizza segnali deboli, identifica pattern di non conformità e suggerisce interventi correttivi prima che emergano violazioni.

Algoritmi di *natural language processing* monitorano in tempo reale le evoluzioni normative; sistemi di *anomaly detection* individuano comportamenti atipici nei processi; strumenti di *machine learning* correlano eventi e indicatori per stimare il rischio residuo. La funzione Compliance diventa così un **centro di intelligenza preventiva,** capace di orientare strategia e innovazione.

In questa prospettiva, la regolamentazione non è più una risposta al rischio, ma un **alleato della trasformazione.** La governance intelligente nasce quando la tecnologia non è solo oggetto di controllo, ma parte integrante del suo esercizio: un modello in cui **Risk, Audit e Compliance** lavorano insieme per garantire **fiducia, trasparenza e progresso sostenibile**, in coerenza con i principi introdotti dall'**AI Act[3] e dal DORA Regulation[4].**

6. Il nostro approccio ERM-AI e gli acceleratori di Risk AI nel contesto italiano

6.1. ERM-AI: il nostro approccio al rischio aziendale

Per Enterprise Risk Management (ERM) si intende un approccio strutturato e integrato alla gestione dei rischi aziendali, considerati nella loro globalità. L'ERM consente di identificare, valutare, mitigare e monitorare in modo proattivo minacce e opportunità, riducendo l'incertezza e aumentando la resilienza dell'organizzazione. Favorisce la limitazione delle perdite economiche, operative e reputazionali, migliora la qualità delle decisioni, ottimizza l'allocazione delle risorse e rafforza la fiducia degli stakeholder, dimostrando responsabilità e conformità normativa.

La nostra esperienza nello sviluppo e nell'aggiornamento di modelli ERM per organizzazioni di settori diversi ci ha portato a elaborare un approccio che chiamiamo ERM-AI: una naturale evoluzione dell'Enterprise Risk Management che integra le potenzialità dell'Intelligenza Artificiale.

Non si tratta di una metodologia tecnica destinata esclusivamente agli specialisti, ma di un approccio sufficientemente flessibile da adattarsi alle esigenze specifiche di ogni azienda, indipendentemente dalla sua dimensione o settore. L'idea che ci guida è quella di rendere la gestione del rischio evoluta accessibile a tutte le organizzazioni, comprese quelle di medie e piccole dimensioni, superando le barriere tradizionali di complessità e costo attraverso l'uso consapevole dell'AI.

Questo approccio si fonda su cinque principi che rappresentano la sintesi della nostra visione e della nostra esperienza nel campo del Risk Management.

ERM-AI: I cinque principi cardine

1. Anticipare, non reagire: il valore della proattività

In un mondo in rapida evoluzione, la gestione reattiva del rischio è come guidare guardando solo lo specchietto retrovisore. Un approccio proattivo significa invece leggere i segnali deboli, anticipare le discontinuità e integrare il rischio nella strategia aziendale come fattore di orientamento. Questo cambio di prospettiva porta benefici concreti: riduzione delle perdite, ottimizzazione delle risorse, maggiore fiducia degli stakeholder e, soprattutto, la capacità di trasformare l'incertezza in opportunità di innovazione. La conformità normativa diventa così non un vincolo, ma una conseguenza naturale di una gestione consapevole.

1. L'Intelligenza Artificiale come amplificatore umano

L'AI sta ridefinendo i confini del possibile nel Risk Management. Non si tratta solo di automatizzare le attività ripetitive o velocizzare i processi, ma di rendere accessibili capacità analitiche prima riservate a poche grandi organizzazioni. L'AI consente di prevedere pattern nascosti, monitorare rischi in tempo reale e garantire una compliance dinamica. Ma questa potenza porta con sé nuove responsabilità: le sfide etiche e normative dell'AI vanno affrontate con la stessa serietà con cui ne sfruttiamo le potenzialità. Per questo abbiamo sviluppato H2RAI, che garantisce che ogni applicazione di AI nel Risk Management rispetti i più alti standard di affidabilità, trasparenza e conformità.

2. La cultura del rischio come intelligenza collettiva

Una tecnologia, per quanto avanzata, è efficace solo quanto la cultura che la sostiene. La gestione del rischio non può essere confinata a una funzione o a un software: deve permeare l'intera organizzazione, dal board agli operativi. Costruire una cultura del rischio significa coinvolgere ogni livello aziendale nel riconoscere, comunicare e gestire proattivamente le incertezze. La formazione continua trasforma la consapevolezza individuale in intelligenza collettiva, rendendo il Risk Management parte naturale dei processi decisionali quotidiani.

4. Governance integrata: superare i silos organizzativi

Il rischio non rispetta i confini organizzativi. Una governance efficace richiede che le diverse funzioni aziendali - finance, IT, compliance, operations - parlino lo stesso linguaggio e condividano la stessa visione. Questo significa definire ruoli chiari, creare comitati trasversali e stabilire processi che connettano invece di separare. La trasparenza e la comunicazione tempestiva diventano così non solo strumenti di controllo, ma fondamenta della fiducia interna ed esterna. È la fine dell'approccio a silos: il rischio diventa materia di governo condiviso.

5. Dal Risk Management al Risk Leadership: creare valore strategico

Integrare il Risk Management nella strategia aziendale significa riconoscere che ogni decisione contiene un elemento di incertezza e che questa incertezza, se ben gestita, può diventare fonte di vantaggio competitivo. Non si tratta solo di proteggere l'esistente, ma di abilitare la crescita sostenibile. Le crisi nascondono opportunità, le discontinuità aprono nuovi mercati, i vincoli stimolano l'innovazione. Un approccio strategico al rischio prepara l'organizzazione non solo a resistere agli shock, ma a emergerne più forte e adattiva.

6.2. Gli acceleratori di NTT DATA: H2RAI e Osservatorio Normativo AI

Come anticipato, NTT DATA non si è limitata a sviluppare un approccio di **Enterprise Risk Management** (ERM-AI), ma ha creato anche due acceleratori innovativi: **H2RAI e Osservatorio Normativo AI**.

H2RAI è il cuore metodologico dei nostri sviluppi AI. Questa metodologia consente a tutte le organizzazioni di sfruttare appieno le potenzialità dell'intelligenza artificiale nelle diverse attività di business, garantendo fin dalle prime fasi di sviluppo del sistema il rispetto dei più elevati standard di affidabilità e delle normative e linee guida etiche più rigorose.

Osservatorio Normativo AI è il primo acceleratore proprietario sviluppato secondo i rigorosi requisiti H2RAI. Affronta la sfida della volatilità normativa aggiornando in tempo reale le novità regolatorie rilevanti per il business, integrandole nei modelli di rischio aziendali e generando scenari di stress test per verificarne la resilienza.

Questi acceleratori rappresentano la traduzione concreta dei principi ERM-AI: non sostituiscono i processi esistenti, ma li potenziano con strumenti digitali che rendono la gestione dei processi aziendali e del risk management più rapida, misurabile e sostenibile. La logica sottostante non è quella di imporre nuove procedure, ma di amplificare le capacità esistenti attraverso l'intelligenza artificiale, mantenendo sempre l'uomo al centro del processo decisionale.

6.3. H2RAI: la potenza dell'AI sotto controllo

H2RAI (Human to Responsible AI) rappresenta la sintesi operativa della nostra visione: come possiamo sfruttare le straordinarie potenzialità dell'AI senza perdere di vista la responsabilità che questa comporta? La risposta non è nel limitare l'innovazione, ma nel governarla consapevolmente, analizzando e mitigando i rischi fin dalle prime fasi di sviluppo.

Questa metodologia nasce dall'esperienza maturata in progetti di Enterprise Risk Management, Audit digitale e AI Governance nei principali settori regolati — dalla finanza all'energia, dalla pubblica amministrazione alla sanità. Ogni progetto ha contribuito a raffinare un approccio che risponde a una domanda cruciale: come rendere l'AI non solo oggetto di controllo, ma parte integrante del sistema di governance stesso?

H2RAI unisce principi di responsabilità, strumenti di controllo e processi di validazione in un framework operativo che dialoga naturalmente con il Regolamento AI Act (UE 2024/1689)[3], il DORA (UE 2022/2554)[4], lo standard ISO 31000:2018[1] e le linee guida EBA/EIOPA[6],[7]. Non si tratta di sovrapporre un ulteriore livello di complessità ai modelli esistenti, ma di creare connessioni, offrendo una piattaforma che evolve insieme alla maturità organizzativa.

I cinque capisaldi di H2RAI

1. Responsabilità e trasparenza

Ogni sistema di AI deve essere come un libro aperto: tracciabile nelle sue decisioni, auditabile nei suoi processi, supervisionato nei suoi risultati. L'intelligenza umana resta il fulcro — non per diffidenza verso la macchina, ma per la consapevolezza che solo l'uomo può attribuire significato etico alle decisioni.

2. Etica by design

L'etica non è un ripensamento post-sviluppo, ma il DNA stesso del sistema. Ogni modello viene concepito considerando fin dall'inizio i suoi impatti — sociali, ambientali, umani. È la differenza tra costruire una tecnologia che funziona e una che funziona responsabilmente.

3. Supervisione umana

I meccanismi di controllo sono calibrati sul livello di rischio, seguendo il principio di proporzionalità dell'AI Act[3]. Maggiore è l'impatto potenziale, più stringente è la supervisione — non come freno, ma come garanzia di affidabilità.

4. Auditabilità e tracciabilità

Ogni decisione lascia un'impronta digitale, ogni dataset racconta la sua storia. La documentazione non è burocrazia, ma memoria organizzativa — la possibilità di comprendere, verificare e migliorare continuamente.

5. Valore sostenibile

Il Risk Management dell'AI non si esaurisce nell'evitare sanzioni o non conformità. Il suo scopo più alto è creare fiducia duratura e valore economico di lungo periodo — trasformare la compliance in competitività.

Questi principi costituiscono la **spina dorsale del modello H2RAI**, pensato per integrare Risk, Audit e Compliance in un linguaggio comune di responsabilità condivisa.

6.3.1. Come funziona H2RAI: il modello Stage & Gate

Il framework H2RAI è organizzato in un modello a fasi successive (Stage & Gate), che consente di **valutare, approvare e monitorare** i sistemi di AI lungo l'intero ciclo di vita.

1. Ideation Stage

Il punto di partenza è sempre la domanda: questo uso dell'AI è coerente con i nostri valori, la nostra strategia, le normative vigenti? È qui che si pongono le fondamenta etiche del progetto realizzando l'analisi preliminare del caso d'uso, la valutazione di coerenza con strategia, i regolamenti e principi etici.

2. Design Stage

I principi diventano architettura. Si definiscono i dataset, si progettano le metriche per identificare potenziali bias, si stabiliscono i requisiti di spiegabilità. L'AI by design prende forma concreta applicando i principi di AI by Design attraverso la definizione di dataset, le metriche di bias e i requisiti di explainability.

3. Development Stage

La costruzione procede sotto controllo continuo: il versioning dei modelli, la validazione tecnica, i test documentati. Ogni passo è tracciato, ogni scelta registrata attraverso anche il controllo dei dati.

4. Deployment Gate

Il momento della verità. Prima del rilascio, una revisione completa verifica la conformità (AI Act[3], GDPR, DORA[4], EBA[6], EIOPA[7]) e linee guida di settore. Solo se tutti i requisiti sono soddisfatti, il sistema può entrare in produzione.

5. Monitoring Stage

L'AI vive e apprende, e con essa deve evolvere il controllo. Meccanismi di early warning, analisi continua degli impatti, reporting automatico: la governance accompagna il sistema per tutto il suo ciclo di vita.

Ogni fase prevede checklist dedicate, punti di controllo e reportistica integrata con il sistema di gestione del rischio aziendale. La logica *Stage & Gate* consente di **tracciare le decisioni e intervenire tempestivamente** in caso di deviazioni, garantendo una governance verificabile e conforme.

6.3.2. H2RAI: Applicazioni settoriali

H2RAI è pensato per essere **scalabile e adattabile** a contesti regolatori diversi. La sua logica è sempre la stessa — *anticipare, validare, monitorare* — ma le priorità cambiano a seconda del settore:

• **Finance:** gestione dei modelli di scoring o antifrode in conformità con **AI Act**[3] e linee guida **EBA**[6].

• **Energy & Utilities:** validazione etica e operativa dei sistemi di previsione della domanda e delle reti intelligenti, in coerenza con **DORA**[4].

• **Healthcare:** garanzia di trasparenza e tracciabilità per AI diagnostiche o di supporto clinico.

• **Manifatturiero:** controllo predittivo dei processi di manutenzione e qualità, con metriche di explainability.

• **Pubblica Amministrazione:** audit delle decisioni automatizzate, con principi di equità e supervisione umana.

Ogni implementazione è accompagnata da un percorso di **assessment iniziale e formazione**, volto a sensibilizzare i team aziendali sui rischi e le opportunità dell'AI Governance.

6.3.3. H2RAI: Benefici

L'adozione di H2RAI porta benefici che vanno oltre la conformità normativa e non rappresenta solo una metodologia, ma una filosofia operativa. L'adozione del framework H2RAI consente di:

• **integrare risk, audit e compliance** in un unico sistema coerente;

• **ridurre i tempi di verifica e reporting**, grazie all'automazione delle checklist;

• **garantire tracciabilità e trasparenza**, conformemente ai requisiti regolatori [3,4,6,7];

• **migliorare la reputazione** e la fiducia degli stakeholder, grazie a una governance verificabile.

Dal punto di vista operativo, la metodologia crea **continuità tra prevenzione e innovazione**: ogni nuovo progetto di AI nasce già dotato di strumenti di conformità e monitoraggio, riducendo il rischio di implementazioni opache o non etiche.

H2RAI rappresenta quindi una **nuova frontiera della consulenza Risk & Compliance**: un approccio pragmatico, scalabile e responsabile, che unisce esperienza, metodo e visione.

Riassumendo, il framework H2RAI non è un modello teorico, ma una **proposta evolutiva basata su esperienze reali** rappresentando la traduzione concreta del principio cardine di tutto il documento: **governare l'AI per rendere il rischio una leva di fiducia e valore sostenibile**.

6.4. Osservatorio Normativo AI: Anticipare i cambiamenti normativi

La volatilità normativa rappresenta una delle principali fonti di incertezza per chi deve prendere decisioni strategiche, specialmente quando si tratta di tecnologie emergenti[3,4,6,7]. I modelli tradizionali di risk management faticano a integrare questa dimensione dinamica, limitandosi spesso a valutazioni periodiche che rischiano di diventare obsolete in un contesto regolatorio in continua evoluzione.

L'Osservatorio Normativo AI di NTT DATA nasce per trasformare questa incertezza normativa in rischio quantificabile e gestibile, applicando l'intelligenza artificiale a un problema che tradizionalmente richiedeva enormi risorse umane. A differenza dei tradizionali servizi di monitoraggio normativo, l'Osservatorio non si limita a segnalare i cambiamenti ma:

• **trasforma** i segnali regolatori deboli in analisi probabilistiche di impatto, utilizzando modelli predittivi addestrati su basi di dati di evoluzione normativa storica

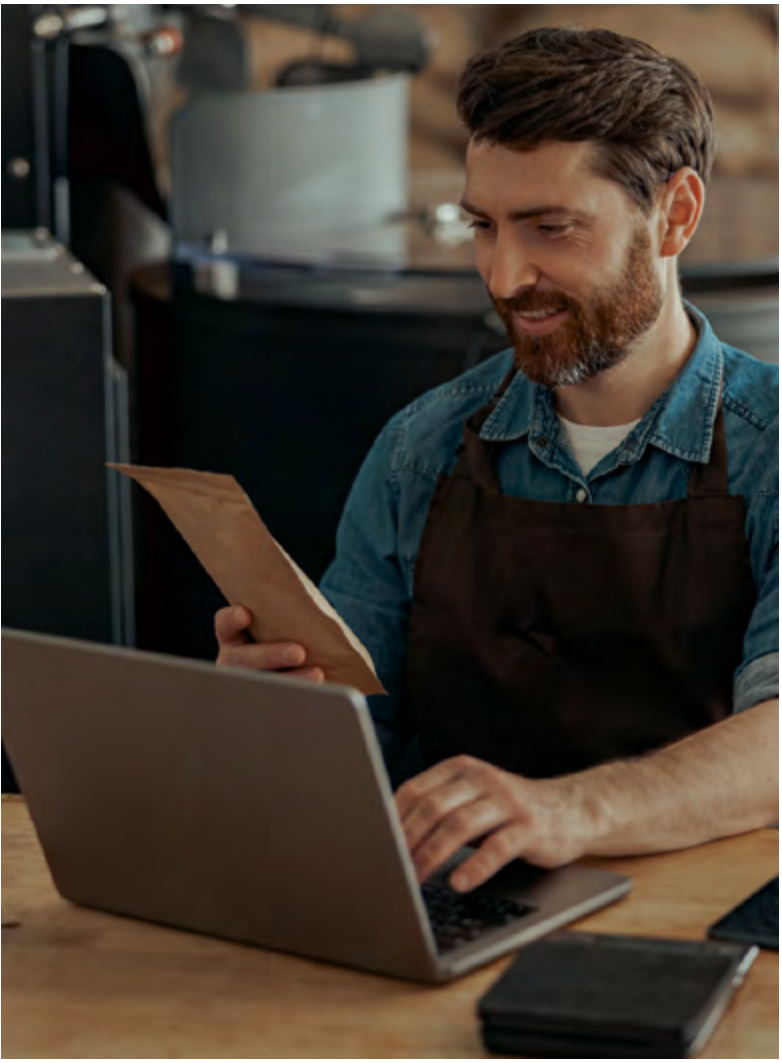
• **integra** automaticamente gli sviluppi normativi nei modelli di rischio esistenti, aggiornando in tempo reale i profili di rischio delle iniziative aziendali

• **genera** scenari di stress-test normativi per validare la

resilienza delle strategie aziendali rispetto a potenziali cambiamenti regolatori

L'architettura tecnologica dell'Osservatorio si basa su tre componenti principali: **modelli di elaborazione** del linguaggio naturale specializzati nell'analisi di testi legali e regolatori; sistemi di Intelligenza Artificiale **addestrati sul contesto normativo specifico** di ogni settore; e **grafi di conoscenza** che mappano le interdipendenze tra normative, processi aziendali e asset strategici. Questa combinazione permette non solo di identificare i cambiamenti, ma di comprenderne le implicazioni sistemiche.

L'Osservatorio incarna concretamente i principi del nostro approccio al risk management: **l'approccio proattivo** si traduce nell'anticipare sviluppi normativi prima della loro formalizzazione; **l'AI al centro** significa automatizzare l'analisi di volumi di informazioni impossibili da gestire manualmente; **la governance integrata** connette direttamente gli insight normativi ai processi decisionali aziendali.



Ma il valore più profondo sta nel restituire alle persone il controllo sull'incertezza normativa. I **risk manager**, i **compliance officer** e i **decisori strategic**i possono finalmente passare dal rincorrere i cambiamenti all'anticiparli, dal subire la complessità normativa al governarla. L'Osservatorio diventa così non solo uno strumento tecnologico, ma un abilitatore di quella cultura del rischio proattiva di cui abbiamo parlato.

Questo acceleratore, primo nato secondo i rigorosi requisiti H2RAI, dimostra come l'intelligenza artificiale possa essere applicata per gestire le sfide stesse che la sua adozione comporta. È la dimostrazione concreta che la tecnologia, quando governata responsabilmente, può trasformare anche l'incertezza più complessa in conoscenza utile e azionabile.

Grazie all'Osservatorio Normativo AI, la funzione di Risk Management evolve da presidio reattivo a piattaforma cognitiva capace di apprendere dal contesto e orientare le decisioni strategiche. Ogni aggiornamento normativo diventa un'opportunità di miglioramento, ogni variazione regolatoria una fonte di vantaggio competitivo.

L'Osservatorio non è solo un sistema di monitoraggio, ma un vero e proprio ecosistema di intelligenza normativa, in cui l'AI analizza, correla e anticipa, mentre l'uomo interpreta, decide e dà significato. In questo dialogo tra algoritmo e giudizio umano nasce la nuova frontiera della compliance predittiva, in cui la conoscenza regolatoria diventa parte integrante del governo d'impresa.

È così che NTT DATA traduce il principio "Human to Responsible AI" in pratica quotidiana: riportando la responsabilità al centro dell'innovazione e offrendo alle organizzazioni strumenti per affrontare l'evoluzione normativa non come minaccia, ma come leva di fiducia e sostenibilità."

6.5. La democratizzazione del Risk Management: opportunità per le PMI italiane

Per la prima volta nella storia del Risk Management, la distanza tra grandi e piccole organizzazioni si sta riducendo. L'Intelligenza Artificiale, insieme ai modelli cloud e as-a-service, sta abbattendo quelle barriere di costo e complessità che tradizionalmente relegavano gli strumenti predittivi avanzati alle sole grandi corporation. È un cambiamento che tocca il cuore del tessuto produttivo italiano, dove le PMI rappresentano non l'eccezione ma la regola.

Questo processo di democratizzazione tecnologica è al centro del nostro approccio **ERM-AI**: non si tratta solo di rendere disponibili strumenti sofisticati, ma di ripensare come questi strumenti possano adattarsi alle reali esigenze e capacità delle organizzazioni di ogni dimensione. Una PMI manifatturiera non ha bisogno degli stessi modelli di una multinazionale, ma ha diritto alla stessa capacità di leggere e anticipare i rischi che la riguardano.

H2RAI gioca un ruolo fondamentale in questo processo. Attraverso modelli scalabili e processi calibrati sul livello di rischio effettivo, anche le organizzazioni con risorse limitate possono integrare pratiche avanzate di risk management senza investimenti proibitivi o competenze iperspecialistiche. L'automazione intelligente di raccolta dati, analisi e reporting libera tempo e risorse che possono essere dedicate a ciò che nessuna macchina può fare: valutare il contesto, prendere decisioni etiche, costruire relazioni di fiducia.

È importante sottolineare che la tecnologia amplifica ma non sostituisce. L'AI può identificare pattern, segnalare anomalie, proporre correlazioni, ma la valutazione finale — cosa costituisce un rischio accettabile, quali valori proteggere, come bilanciare opportunità e prudenza — resta saldamente nelle mani delle persone.

La supervisione umana non è un limite della tecnologia: è la garanzia della sua affidabilità.

In Italia, con un tessuto produttivo dominato dalle PMI, questa evoluzione rappresenta un'opportunità di sistema. I dati del CINEAS – Osservatorio di Risk Management 2025[13] mostrano come le imprese che adottano strumenti digitali di governance del rischio registrino migliori performance in termini di continuità operativa e capacità di risposta alle crisi. Ma la vera trasformazione non è solo tecnologica: è culturale. La democratizzazione del Risk Management significa rendere la consapevolezza del rischio parte del DNA imprenditoriale italiano. Significa che un'azienda familiare può accedere a strumenti predittivi prima impensabili, che una start-up può costruire la propria strategia su basi analitiche solide, che un distretto produttivo può condividere pratiche e conoscenze attraverso piattaforme collaborative.

Quando questa evoluzione sarà completata — e i segnali indicano che il processo è già in corso — avremo non solo imprese più resilienti, ma un intero ecosistema economico capace di trasformare l'incertezza in vantaggio competitivo. È questa la promessa della democratizzazione: non livellare verso il basso, ma elevare tutti verso l'alto.

7. Conclusioni

Il Risk Management non è più soltanto un insieme di controlli: è il codice sorgente della fiducia. In un mondo in cui l'Intelligenza Artificiale ridisegna i confini del rischio e della decisione, la governance non può limitarsi a vigilare — deve comprendere, guidare e anticipare. La vera trasformazione non è tecnologica, ma culturale: passare da una logica di reazione a una di consapevolezza.

Questa idea trova la sintesi perfetta nel nostro approccio all'Enterprise Risk Management **ERM-AI**, fondato su cinque principi pratici imprescindibili, maturati attraverso la nostra esperienza nel risk management e applicati in ogni progetto, indipendentemente da dimensione o settore: approccio proattivo, AI al centro, cultura del rischio, governance integrata e strategia aziendale.

L'AI rende la gestione del rischio più veloce, analitica e precisa, ma la sua efficacia dipende da un principio antico: la **responsabilità del giudizio umano**. I modelli calcolano, ma non comprendono il contesto, le reti neurali imparano, ma non decidono che cosa è giusto. Per questo il Risk Management del futuro sarà definito non dalla potenza delle macchine, ma dalla capacità delle persone di **dare significato alle decisioni automatizzate**.

Nel nuovo equilibrio tra tecnologia e coscienza, NTT DATA propone con **H2RAI – Human to Responsible AI** una visione di governance che mette l'etica al centro dell'innovazione. Un modello che integra Risk, Audit e Compliance in un ecosistema trasparente, dove la responsabilità è condivisa e la fiducia è costruita come infrastruttura. Il Risk Management non è più una funzione di controllo, ma un **tessuto connettivo tra strategia, innovazione e fiducia**.

In questo contesto emergono tre protagonisti della governance del futuro:

• Il **CRO**, che interpreta i segnali del rischio e li trasforma in conoscenza.

• Il **CEO**, che ne fa leva per orientare la visione strategica e il valore sostenibile.

• Il **CIO**, che diventa il custode del nuovo equilibrio tra intelligenza umana e Intelligenza Artificiale — l'**architetto della fiducia digitale**. Il suo ruolo non è più solo tecnologico, ma culturale: assicurare che l'innovazione resti tracciabile, spiegabile e allineata ai principi etici dell'impresa.

Il Risk Management, la tecnologia e la leadership convergono così in una stessa direzione: governare la complessità per generare fiducia.

7.1. Prospettive al 2035

Guardando al 2035, la gestione del rischio sarà una disciplina ibrida, a metà tra **intelligenza predittiva e coscienza etica**. Le organizzazioni saranno sistemi adattivi, capaci di apprendere dal contesto e di prevenire le vulnerabilità in modo autonomo. Il quantum leap del Risk Management non consisterà nel prevedere tutto, ma nel **scegliere cosa mantenere umano**: la decisione, il valore, la fiducia.

Il **CIO del futuro** sarà il mediatore di questo ecosistema, l'interprete del linguaggio tra algoritmi e persone. Non gestirà solo infrastrutture, ma **ecosistemi cognitivi**: piattaforme in cui la sicurezza, la trasparenza e l'etica saranno progettate come parte nativa dei sistemi. Insieme al CRO e al CEO, diventerà garante di una governance evolutiva in cui il rischio è compreso, non temuto; controllato, ma anche utilizzato come leva per innovare.

Nel 2035, il Risk Management evolverà in **Risk Intelligence**: una rete di decisioni distribuite, in cui l'uomo e la macchina condividono responsabilità e visione. Il **CIO** progetterà infrastrutture di fiducia, il **CRO** modellerà il rischio come vantaggio competitivo, mentre il **CEO** avrà il compito di orientare la cultura aziendale verso la trasparenza e la sostenibilità.

Forse, la più grande innovazione del prossimo decennio non sarà l'AI in sé, ma la **coscienza collettiva che sapremo costruire attorno a essa**. Quando la tecnologia sarà al servizio del significato e la fiducia diventerà il nuovo capitale strategico, potremo dire di aver realizzato il vero salto quantico del Risk Management.

Il futuro della governance non sarà scritto dal codice, ma da chi saprà trasformarlo in coscienza.

8. Dalla teoria all'impatto: esperienze reali di Risk Management con H2RAI

Case study 1:

Energia predittiva e fiducia algoritmica – L'AI al servizio delle Utilities

Nel 2024, una grande azienda italiana del settore energia e utilities ha avviato un ambizioso percorso di trasformazione digitale per migliorare l'efficienza operativa e l'esperienza dei clienti. NTT DATA ha accompagnato l'organizzazione nell'integrazione di soluzioni di Intelligenza Artificiale progettate secondo i principi di H2RAI, garantendo un equilibrio costante tra innovazione, compliance e responsabilità.

Il progetto è partito da un ampio coinvolgimento degli stakeholder interni — dai team IT e Customer Experience alle Risorse Umane — per mappare i bisogni e definire le aree di maggiore impatto. Da questa analisi sono emerse cinque priorità: una piattaforma conversazionale multicanale per i clienti; un assistente virtuale interno a supporto dei dipendenti; una soluzione di AI per il matching dei CV; un motore di analisi automatica dei report ESG; un assistente per il service desk integrato con i sistemi IT aziendali. Tutte le soluzioni sono state progettate per integrarsi nei processi esistenti, migliorando tempi di risposta e qualità del servizio.

L'adozione di H2RAI ha assicurato che ogni sistema fosse sviluppato e monitorato nel rispetto dei principi di trasparenza, auditabilità e supervisione umana. Ogni fase, dal design al rilascio, è stata validata secondo i requisiti dell'AI Act e degli standard ISO 31000, garantendo tracciabilità e conformità.

I risultati sono tangibili: la riduzione media del 10% delle attività ripetitive ha liberato tempo per attività a maggiore valore strategico, mentre la qualità del servizio è cresciuta grazie alla maggiore coerenza e velocità dei processi automatizzati. Ma il valore più importante è culturale: l'azienda ha sviluppato una nuova consapevolezza del rischio algoritmico, imparando a governare l'AI come leva di fiducia e non solo di efficienza.

Il caso dimostra come H2RAI possa tradurre la complessità tecnologica e normativa in valore operativo concreto, rendendo la governance dell'AI un fattore di competitività sostenibile anche in settori altamente regolati come quello energetico.

Case study 2:

Gestire il rischio con intelligenza: Project Risk Management

Nel 2024 una grande azienda italiana ha avviato la revisione dei propri strumenti di **Project Risk Management (PRM)**. Nonostante disponesse di piattaforme avanzate per simulazioni complesse, il sistema in uso non era più integrato nell'ecosistema aziendale e non rispondeva alle nuove esigenze di scala e sicurezza. Per evitare un impatto su budget, scheduling e continuità operativa, l'azienda si è rivolta a **NTT DATA** per un progetto di rinnovamento fondato su prevenzione, Intelligenza Artificiale e governance etica.

Il primo passo è stato l'ascolto: stakeholder tecnici e responsabili di Risk Management hanno contribuito a definire i requisiti funzionali e IT del nuovo strumento. È stato progettato un **risk register unificato**, con gestione centralizzata dei rischi, stime qualitative e quantitative e simulazioni basate su **algoritmi Monte Carlo**. Abbiamo inoltre integrato un modello avanzato di analisi dati a supporto delle simulazioni, rendendo il processo più accurato e tempestivo.

Elemento distintivo del progetto è stato l'impiego della metodologia **H2RAI**, che ha assicurato la **compliance normativa ed etica** in tutte le fasi del processo, dal design alla supervisione dei modelli. H2RAI ha garantito la coerenza con i principi del Digital Operational Resilience Act (DORA) e dell'AI Act, rafforzando la fiducia nei sistemi automatizzati.

Grazie alla combinazione di competenze tecnologiche e metodologiche, **NTT DATA** ha guidato la selezione delle soluzioni PRM più performanti e compatibili con l'infrastruttura esistente, assicurando sicurezza, trasparenza e proattività.

Il risultato è stato duplice: un nuovo modello di Project Risk Management, conforme ai più elevati standard di settore, e una **cultura del rischio più matura**, orientata alla prevenzione e alla governance intelligente. Un esempio concreto di come **H2RAI** traduca la complessità normativa e tecnologica in valore operativo, rendendo la gestione del rischio una leva di competitività sostenibile.

Case study 3:

Democratizzare l'AI nella farmaceutica: dalla teoria all'impatto

Una media azienda farmaceutica italiana ci ha chiesto supporto per introdurre l'AI nei propri processi con un approccio responsabile, pur non avendo le risorse di una multinazionale. Con circa 800 dipendenti e la sfida di competere in un mercato sempre più data-driven, rappresentava il tessuto produttivo tipico delle PMI italiane che rischiano di restare ai margini della trasformazione digitale. La risposta è stata **H2RAI**.

Il percorso è partito dalle persone. Attraverso workshop mirati abbiamo aiutato l'organizzazione a comprendere non solo le opportunità dell'AI, ma anche i dilemmi etici: quando fidarsi di un algoritmo? Come bilanciare automazione e responsabilità? Leadership e management hanno lavorato su accountability e trasparenza, mentre i team operativi si sono concentrati sulla supervisione umana degli strumenti AI.

La svolta è arrivata con l'implementazione di un **sistema di farmacovigilanza predittiva**, scelto tra oltre quaranta processi. Il sistema analizza segnali deboli provenienti da social media, forum e letteratura scientifica per individuare potenziali eventi avversi, ma ogni segnalazione è **accompagnata da una spiegazione e validata da un farmacista**: l'AI amplifica l'intelligenza umana, non la sostituisce.

È nata così una **governance adattiva**, con un Comitato Etico AI trasversale, processi di audit trasparenti e meccanismi di feedback continuo. Non una burocrazia in più, ma un sistema che apprende e si adatta, riflettendo i principi di H2RAI.

Il risultato più importante è culturale: l'azienda ha sviluppato una **cultura del rischio**, leggendo l'AI come strumento da governare con consapevolezza. Oggi gestisce i rischi algoritmici con strumenti e processi prima riservati alle big pharma, dimostrando che il risk management avanzato è accessibile anche alle PMI se supportato da un **metodo rigoroso e human-centered**.

Questo caso conferma la tesi del nostro position paper: la trasformazione del Risk Management attraverso l'AI non è teoria, ma realtà implementabile — a condizione di mantenere l'uomo al centro della rivoluzione tecnologica.

Case study 4:

Verso un modello di Risk Management data-driven e responsabile

Recentemente un'importante azienda italiana, articolata in diverse business unit e impegnata in progetti di elevata complessità tecnologica e organizzativa, ha avviato una revisione dei propri strumenti di Enterprise Risk Management, ritenuti ormai datati e poco integrati con l'ecosistema informativo aziendale. L'obiettivo dell'iniziativa era individuare una piattaforma più moderna, scalabile e in grado di sfruttare in modo responsabile le potenzialità dell'Intelligenza Artificiale, garantendo al tempo stesso piena conformità con i requisiti normativi e le best practice internazionali di governance del rischio.

Consapevole della strategicità e della sensibilità del progetto, l'azienda ha scelto di affidarsi a NTT DATA per la propria esperienza nel campo del risk management e delle tecnologie AI applicate ai processi aziendali. L'approccio metodologico H2RAI si è rivelato determinante per impostare un piano di modernizzazione etico, sicuro e centrato sull'uomo, in linea con i principi di responsabilità, trasparenza e controllo umano che guidano l'adozione dell'AI nei contesti critici.

Il progetto è stato avviato con un'analisi approfondita del sistema ERM esistente, realizzata in collaborazione con il fornitore della soluzione in uso, per individuare criticità e aree di miglioramento tecnico e funzionale.

In parallelo è stata condotta una mappatura dei processi operativi e delle esigenze evolutive dell'organizzazione, supportata da interviste a figure chiave come il responsabile ERM e i referenti IT. Dalle interviste è emersa con chiarezza l'esigenza di una piattaforma più integrata con l'ecosistema informativo aziendale e capace di supportare simulazioni predittive sui rischi, anche complessi, sfruttando l'AI come leva di analisi e prevenzione.

Rispondendo alle legittime preoccupazioni del cliente in materia di compliance e responsabilità, NTT DATA ha proposto l'adozione del framework H2RAI, che assicura l'applicazione dei principi di AI responsabile lungo tutto il ciclo di vita della soluzione — dalla progettazione all'implementazione fino al monitoraggio continuo — garantendo coerenza con il quadro normativo europeo, inclusi l'AI Act e il GDPR. Tale approccio ha permesso di impostare sin dall'inizio un modello di sviluppo controllato, che prevede la supervisione umana nei punti decisionali critici e un'attenzione costante alla tracciabilità e all'auditabilità delle decisioni algoritmiche.

Sulla base dell'analisi tecnica e delle informazioni raccolte, il team ha redatto un documento dettagliato dei requisiti funzionali e non funzionali della futura piattaforma ERM. Come riferimento metodologico è stato adottato il COSO ERM Framework, standard internazionale riconosciuto per la gestione integrata dei rischi e per l'allineamento dei processi di controllo interno alla strategia aziendale. Questo ha consentito di assicurare coerenza tra l'evoluzione tecnologica del sistema e i principi di governance e accountability che guidano l'organizzazione.

Il progetto si è concluso con la consegna del documento dei requisiti e con un percorso di accompagnamento che ha permesso al cliente di sviluppare una maggiore consapevolezza sui benefici e sulle cautele necessarie nell'introduzione di componenti di Intelligenza Artificiale nei processi di gestione del rischio. L'iniziativa ha gettato le basi per una modernizzazione sostenibile dell'intero sistema ERM, rafforzando la capacità dell'azienda di anticipare i rischi e di prendere decisioni basate su dati in modo conforme, etico e tracciabile.

L'efficacia dell'intervento è derivata dalla combinazione tra l'approccio metodologico di NTT DATA al risk management — fondato su principi di responsabilità, etica by design e supervisione umana — e l'applicazione dell'acceleratore H2RAI, che ha assicurato la conformità tecnica, normativa e valoriale delle soluzioni proposte. Il risultato finale è un modello di governance del rischio data-driven, pronto a integrare l'AI in modo sicuro e trasparente e a rafforzare il ruolo del fattore umano come garante ultimo di affidabilità e fiducia.

9. Note e Riferimenti bibliografici

[1] **ISO – International Organization for Standardization** (2018). *ISO 31000: Risk Management – Guidelines.* Ginevra: ISO.

[2] **CoSO – Committee of Sponsoring Organizations of the Treadway Commission** (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.*

[3] **Unione Europea** (2024). *Regolamento (UE) 2024/1689 – Artificial Intelligence Act.* Gazzetta ufficiale dell'Unione Europea, Bruxelles.

[4] **Unione Europea** (2022). *Regolamento (UE) 2022/2554 – Digital Operational Resilience Act (DORA).* Gazzetta ufficiale dell'Unione Europea, Bruxelles.

[5] **Unione Europea** (2022). *Regolamento (UE) 2022/2464 – Corporate Sustainability Reporting Directive (CSRD).* Gazzetta ufficiale dell'Unione Europea, Bruxelles.

[6] **EBA – European Banking Authority** (2024). *Guidelines on Internal Governance.* Londra: European Banking Authority.

[7] **EIOPA – European Insurance and Occupational Pensions Authority** (2025). *Opinion on the Use of Artificial Intelligence in Insurance.* Francoforte: EIOPA.

[8] **Assonime & Università Bocconi** (2024). *Rapporto sulla Governance nelle imprese italiane.* Milano: Assonime / SDA Bocconi School of Management.

[9] **Politecnico di Milano – Osservatorio Artificial Intelligence** (2025). *Rapporto 2025: L'Intelligenza Artificiale in Italia.* Milano: Politecnico di Milano, School of Management.

[10] **ISTAT – Istituto Nazionale di Statistica** (2024). *Imprese e ICT 2024.* Roma: ISTAT.

[11] **Anitec-Assinform** (2025). *Rapporto Il Digitale in Italia 2025.* Milano: Confindustria Digitale / NetConsulting cube.

[12] **CINEAS – Consorzio Universitario per l'Ingegneria nelle Assicurazioni** (2024). *Osservatorio di Risk Management 2024.* Milano: Politecnico di Milano.

[13] **CINEAS – Consorzio Universitario per l'Ingegneria nelle Assicurazioni** (2025). *Osservatorio di Risk Management 2025.* Milano: Politecnico di Milano.

[14] **Allianz Global Corporate & Specialty** (2025). *Allianz Risk Barometer 2025.* Monaco di Baviera: Allianz SE.

[15] **European Commission** (2021). Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence, Bruxelles.

Autore

Luca Pozzoli

Managing Director,
Advisory Services,
NTT DATA Italia

Con oltre 30 anni di esperienza nella consulenza direzionale e trasformazione digitale in settori regolamentati (finanza, energia, utilities), ha sviluppato competenze nell'intersezione tra innovazione tecnologica, Risk Management e governance aziendale.

È ideatore di H2RAI – Human to Responsible AI, framework per l'adozione etica e verificabile dell'intelligenza artificiale nelle organizzazioni. La metodologia garantisce trasparenza, auditabilità e supervisione umana lungo tutto il ciclo di vita dei sistemi AI, applicandosi trasversalmente a processi di business, risk management, compliance e audit.

Ingegnere nucleare di formazione, porta nella consulenza un approccio sistemico alla complessità, con la missione di rendere accessibile l'AI governance responsabile a imprese di ogni dimensione.

"La fiducia si costruisce connettendo mondi diversi"

Il documento è stato realizzato con il contributo di Andrea Allegrini - Business & Digital Advisor