Capitolo 6

Risk management nell'Impresa Estesa AI-driven

Sommario: 1. Il rischio come dimensione costitutiva della strategia. – 2. Dalla tassonomia alla progettazione dei presìdi: categorie di rischio e pratiche di governo. – 3. Rischio ICT: definizione, determinanti e impatto dell'IA oggi. – 4. Princìpi di governo del rischio: soglie, presìdi decisioni. – 5. Risk Management: architettura e implicazioni manageriali. – 6. Dal modello al piano di risk management.

1. *Il rischio come dimensione costitutiva della strategia*

La letteratura manageriale ha progressivamente spostato l'inquadramento del rischio da "variabile esterna da contenere" a componente interna della decisione strategica. In questa prospettiva, la strategia gestisce e configura l'esposizione al rischio, perché ogni opzione competitiva ne incorpora un profilo (di mercato, finanziario, tecnologico, reputazionale) ed un orizzonte temporale entro cui può diventare governabile, oppure si consolida in forme difficilmente reversibili.

Nell'approccio manageriale classico si distingue il rischio dall'incertezza; con rischio si intende l'effetto di fenomeni conosciuti o conoscibili che, quindi, possono essere stimati anche con probabilità statistica prevedendo l'impatto atteso. L'incertezza, invece, deriva da fenomeni non conosciuti e, quindi, non prevedibili; ciò impedisce un calcolo ex ante del loro accadimento e dei conseguenti effetti. Si possono distinguere tre categorie di fenomeni:

- *deterministici*, ovvero dipendenti da condizioni preesistenti e legati da un rapporto di causa – effetto o di tipo sinergico;
- *probabilistici*, derivanti da cause indipendenti tra loro però misurabili;
- *entelechiani*, ovvero fenomeni (naturali, politici, sociali, tecnologici, psicologici) nuovi, esogeni all'impresa, in grado di spezzare l'equilibrio e non facilmente riconducibili a definite circostanze.

Ma qual è il limite che separa l'incertezza dal rischio? Ovvero, quando la *non conoscenza* è il presupposto del danno economico per l'impresa? A tali interrogativi può rispondersi - sia pure non in maniera esaustiva - riferendosi al grado di misurazione dell'evento o meglio dei suoi effetti. Per cui si è in presenza di rischio quando le situazioni di incertezza possono essere misurate (anche ex ante) applicando modelli matematico – statistici; si ha, invece, incertezza assoluta quando non è possibile avere alcuna indicazione segnaletica (Knight, 1921).

Il rischio può considerarsi come una *species* del *genus* dell'incertezza avente la natura del danno economico conseguente all'accadimento di un evento (Hardy, 1931). L'incertezza, così, assumerebbe connotati propri caratterizzati da una sorta

DOI Code: 10.1285/i9788883052507v1p97

di oggettivo impedimento conoscitivo indipendente dalle capacità del soggetto osservatore.

Da ciò deriva una conseguenza rilevante per la strategia: la decisione discende dalla capacità di selezione dei rischi accettabili perché misurabili e gestibili cercando anche di ridurre le incertezze attraverso l'apprendimento cognitivo e la capacità di adattamento del sistema (March e Shapira, 1987).

Si ha così passaggio dalla gestione del rischio come attività prevalentemente "di controllo" allo strategic risk management che coincide con un cambio di funzione e di assetto del rischio all'interno dell'impresa. Nell'approccio tradizionale, il rischio è trattato soprattutto come fenomeno da controllare: si identificano minacce, si costruiscono presìdi, si verificano conformità e si interviene quando si manifestano scostamenti. È una logica tipicamente coerente con una concezione del rischio come deviazione rispetto a standard o procedure, quindi governabile tramite regole, auditing e controlli interni. Questa impostazione resta utile e necessaria per i rischi prevenibili, cioè quelli che originano da processi interni e sono riducibili attraverso disciplina organizzativa e compliance (Kaplan e Mikes, 2012). Tuttavia, nei contesti turbolenti e interdipendenti, una parte crescente del rischio non è riducibile a deviazione controllabile: deriva dalle scelte di posizionamento, dalle sfide su tecnologie e mercati, dall'architettura delle dipendenze nell'ecosistema e dalla velocità con cui il contesto evolve.

Lo strategic risk management (SRM) nasce proprio per colmare questo scarto. La sua premessa è che *esiste un rischio "di strategia" che* non può essere semplicemente mitigato senza compromettere la creazione di valore, perché *è incorporato nelle decisioni che generano opportunità*. In questa logica, il rischio diventa una variabile da qualificare e governare cercando di comprendere quali rischi sono accettati intenzionalmente per competere, quali sono incompatibili con la continuità dell'impresa, quali richiedono molta attenzione, opzioni di uscita o capacità dinamiche di adattamento (Kaplan e Mikes, 2012). L'oggetto di governo diventa la configurazione strategica che determina l'esposizione al rischio: scelte di architettura, dipendenze, interfacce operative, regole di delega e velocità di cambiamento. I "fenomeni" sono manifestazioni di tale configurazione; governare il rischio significa intervenire sulle condizioni che rendono probabili certe classi di eventi e sui meccanismi con cui l'organizzazione li intercetta e li contiene.

Un elemento distintivo è, pertanto, rappresentato dalle variabili temporali. Nel risk management di controllo, il tempo è spesso implicito: si assume che il rischio possa essere rilevato e corretto entro cicli di reporting e audit. Nel SRM, invece, tempo e velocità diventano espliciti e considerati nell'orizzonte dell'investimento, nel ritmo di accelerazione del contesto, nella reazione dell'organizzazione e reversibilità delle scelte. Questo è particolarmente rilevante in condizioni di incertezza profonda, quando non è possibile attribuire probabilità affidabili agli esiti perché risultano instabili o non condivise le variabili rilevanti. In questi contesti, la strategia va progettata come percorso adattivo, incorporando

apprendimento continuo, opzioni e revisione delle assunzioni, con punti di decisione attivati da segnali e soglie (Tapinos et al., 2019).

Questo cambio di prospettiva spiega perché ormai sia fondamentale l'integrazione un approccio "enterprise-wide" alla gestione dei rischi, che supera la logica a silos e tratta il rischio come dimensione trasversale dell'organizzazione; quindi, non una funzione separata che interviene ex post, ma un insieme di pratiche e responsabilità che entra nei processi di decisione. Se il rischio strategico è parte della decisione, allora deve essere considerato nel processo decisionale: pianificazione, allocazione del capitale, definizione delle priorità, valutazione delle alternative e monitoraggio delle assunzioni. Il rischio così diventa strategico quando è inseparabile dalle opzioni competitive e quando la sua gestione richiede non solo controlli, ma progettazione di architetture e presìdi che operano prima e durante la formulazione della strategia, non soltanto dopo.

2. *Dalla tassonomia alla progettazione dei presìdi: categorie di rischio e pratiche di governo*

Parlare di "rischio" al singolare è, dunque, fuorviante, perché sotto la stessa etichetta convivono fenomeni diversi per origine, controllabilità ed implicazioni strategiche. La conseguenza manageriale di tale confermato assunto è rilevante: se i rischi non sono omogenei, non può esserlo nemmeno il modo di governarli. In tale prospettiva, possono riconoscersi tre macro ambiti di rischio:

1) *Rischi prevenibili* quelli interni, legati ad errori procedurali, violazioni di policy o fallimenti operativi che, in linea di principio, l'impresa non dovrebbe "accettare" perché non generano valore; la logica di governo appropriata è, quindi, quella della prevenzione tramite regole, controlli, cultura della compliance e sistemi di *internal audit*.
2) *Rischi strategici* rappresentano, invece, il possibile risvolto delle decisioni competitive. In questa tipologia, l'obiettivo non è eliminare il rischio, ma renderlo coerente con obiettivi e capacità dell'impresa, attraverso discussione strategica, definizione di risk appetite, valutazione dei trade-off e progettazione di opzioni di correzione.
3) *Rischi esterni*, infine, comprendono shock macro, eventi geopolitici, discontinuità regolatorie, crisi di filiera o cambiamenti improvvisi nei modelli di business; questi non sono controllabili in origine, quindi, non sono governabili con regole interne richiedono resilienza, piani di continuità e capacità di adattamento rapido.

Questa tassonomia è utile perché rende visibile un possibile bias organizzativo derivante dall'adozione di un unico "stile di controllo" come risposta standard al rischio. Quando le pratiche di governo non sono coerenti con la natura del rischio, si generano tre effetti ricorrenti:

a) irrigidimento della scelta strategica, che riduce lo spazio per sperimentazione e apprendimento;

b) indebolimento dei presìdi su errori ricorrenti, deviazioni procedurali e non conformità, che richiedono invece standard, disciplina operativa e accountability;

c) illusione di controllabilità di fronte a shock esogeni, con investimenti in controlli a basso rendimento e scarso sviluppo di resilienza e capacità di risposta. La tassonomia dei rischi (prevenibili, strategici, esterni) serve, quindi, a collegare categorie di rischio a pratiche di governo appropriate e a preservare l'allineamento tra governance e strategia (Kaplan e Mikes, 2012).

Questo punto si collega direttamente alla prospettiva dell'Enterprise Risk Management (ERM) che fornisce un approccio organizzativo attraverso cui tale logica viene istituzionalizzata, tradotta in processi, responsabilità e flussi informativi continui superando la logica di analisi a silos (finanza, operations, compliance, IT) e considerando il rischio come dimensione trasversale dell'organizzazione (Bromiley et al., 2015). Se il rischio strategico è parte della scelta, allora deve essere considerato nei processi che generano la scelta: pianificazione, allocazione del capitale, definizione delle priorità, valutazione delle alternative e monitoraggio delle assunzioni. Diventa così necessario predisporre un'architettura manageriale che struttura ruoli, procedure e canali informativi affinché le decisioni incorporino sistematicamente valutazioni di rischio. Questa integrazione si realizza anche tramite un linguaggio comune di misurazione: accanto agli indicatori di risultato (KPI), l'ERM introduce *indicatori di rischio* (KRI) che segnalano l'avvicinamento a soglie critiche, rendendo possibile collegare performance e vulnerabilità in modo coerente con priorità di lungo periodo e con i vincoli fissati dalla governance. In tal senso, l'ERM diventa una modalità per progettare e governare la strategia in condizioni di complessità, rendendo espliciti i confini di rischio entro cui la creazione di valore è ritenuta sostenibile (Gordon et al., 2009; Bromiley et al., 2015).

Se la velocità del contesto supera sistematicamente la velocità decisionale dell'impresa, anche una strategia "razionale" sulla carta diventa fragile: l'errore non sta nella scelta iniziale, ma nell'impossibilità di correggerla prima che gli effetti si consolidino. Questo richiede di: rendere esplicite le assunzioni critiche, collegarle a indicatori precoci e prevedere punti di decisione (decision points) in cui, al superamento di determinate soglie, l'impresa modifica intensità, sequenza o direzione della strategia. *Il rischio, quindi, viene incorporato nella strategia perché essa viene progettata come percorso adattivo, non come piano rigido*.

> Si immagini una strategia di crescita basata su una piattaforma digitale esterna, in cui una parte significativa della domanda dipende da *ranking* e *policy* del canale. La scelta può essere profittevole finché l'algoritmo premia determinate pratiche (prezzo, tempi di consegna, investimenti pubblicitari), ma diventa rapidamente negativa se la piattaforma cambia criteri e riduce la visibilità, comprimendo i margini o rendendo non sostenibile il costo di acquisizione cliente. Se l'impresa ha un tempo di reazione breve -perché monitora segnali precoci, ha canali alternativi, può riconfigurare offerta e logistica- il rischio

> resta governabile. Se, invece, il tempo di reazione è lungo -per lock-in tecnologico, dipendenze logistiche o rigidità organizzative- lo stesso cambiamento produce effetti cumulativi prima che l'organizzazione riesca a correggere: perdita di domanda, erosione di cassa, tensioni di filiera. In questo senso, la variabile decisiva non è solo l'evento esterno, ma il rapporto tra velocità del contesto e velocità interna di adattamento, che è esattamente ciò che la letteratura propone di rendere esplicito quando parla di rischio strategico sotto *deep uncertainty*.

Nell'Impresa Estesa questa evoluzione diventa ancora più netta, perché il rischio strategico non coincide più con ciò che accade "dentro" l'organizzazione: nasce e si propaga lungo interfacce, complementarità e dipendenze dell'ecosistema. L'esposizione è legata anche alla struttura della rete (ruoli, colli di bottiglia, nodi critici) ed alla governabilità delle relazioni con attori che controllano risorse decisive (piattaforme, cloud, API, standard, dati). In altri termini, *la strategia deve includere il disegno dell'ecosistema come parte della gestione del rischio, perché il vantaggio competitivo dipende dalla coordinazione di complementi e dall'affidabilità delle interfacce.*

L'adozione dell'IA rende questo quadro bidirezionale: da un lato potenzia la capacità di anticipazione (previsioni, rilevazione anomalie, simulazioni) e definisce il rischio una variabile continua del governo strategico; dall'altro introduce nuove vulnerabilità (opacità, bias, deriva dei modelli, qualità del dato, dipendenza da fornitori, fragilità delle pipeline) che vanno presidiate. Diventa così necessario trattare il rischio dell'IA come rischio organizzativo, non solo tecnico, attraverso funzioni e strumenti di accountability che rendano monitorabili decisioni e sistemi (NIST, 2023; Horneber e Laumer, 2023).

In Europa, inoltre, la cornice regolatoria spinge verso un'integrazione ancora più stretta tra rischio, strategia e governance: l'AI Act introduce un approccio basato sul rischio e obblighi differenziati per sistemi ad alto rischio e per modelli di uso generale, rendendo la "governabilità" dell'IA (documentazione, controlli, supervisione, responsabilità) un elemento che incide direttamente sulle scelte di investimento, di architettura tecnologica e di confine dell'impresa estesa (Regolamento UE 2024/1689).

3. *Rischio ICT: definizione, determinanti e impatto dell'IA*

Il rischio ICT può considerarsi come la probabilità che eventi avversi, interni o esterni, legati a sistemi informativi producano effetti misurabili sulla continuità operativa e sulla capacità dell'impresa di perseguire i propri obiettivi. La sua definizione manageriale coincide con la possibilità che venga compromessa l'utilizzabilità dell'informazione e dei servizi ICT come infrastruttura di esecuzione della strategia. In questo senso, il rischio ICT è una dimensione trasversale del rischio organizzativo, perché l'ICT costituisce oggi il mezzo attraverso cui processi

e coordinamento diventano operatività. Ne deriva che un incidente ICT può generare impatti che possono assumere una rilevanza molto elevata.

La definizione operativa del rischio ICT si declina tradizionalmente lungo tre ambiti fondamentali che definiscono la sicurezza delle informazioni:

- *riservatezza* cioè il rischio di accesso non autorizzato ai sistemi aziendali o di divulgazione impropria e furto di dati sensibili;
- *integrità* ovvero compromissione, manomissione fraudolenta o degrado della qualità dei dati, che rende le informazioni inattendibili e, quindi, distorsive per le decisioni e per i processi che dipendono da quelle informazioni;
- *disponibilità* intesa come malfunzionamento o inefficienza dei sistemi informativi, fino al blocco parziale o totale delle attività operative.

Per comprendere il rischio ICT occorre risalire alle sue determinanti, ricostruendo la sequenza con cui una vulnerabilità o una fragilità organizzativa si trasforma in una causa iniziale e, attraverso meccanismi di propagazione, produce un impatto su processi e asset informativi. L'evento, in assenza di presìdi adeguati, non resta così confinato ma aumenta di rilevanza e di estensione con conseguenze che possono diventare molto rilevanti.

In questa prospettiva, è utile distinguere differenti profili di rischio:

- *applicativo* riguarda il software e il suo ciclo di vita ed è composto da aspetti tecnici e di change management che, quando è debole, genera instabilità sistemica;
- *infrastrutturale* riferito alla base materiale ed alla logica che sostiene i servizi: reti, storage, calcolo, continuità elettrica, data center e piattaforme cloud, insieme alla capacità di backup e ripristino; qui la variabile critica è la possibilità di tornare rapidamente in uno stato operativo con perdita di dati e tempi di fermo compatibili con i processi;
- *cyber security* riguarda invece l'azione intenzionale, esterna o interna, che sfrutta credenziali, privilegi, vulnerabilità note o errori di configurazione per ottenere accesso, muoversi lateralmente, bloccare sistemi, come nei casi di ransomware, botnet o exploit su servizi esposti.

La misurazione del rischio ICT non può fermarsi alla sua fotografia ma necessita di una corretta valutazione per consentire alla governance di decidere come risolvere e prevenire futuri accadimenti.

Diventa fondamentale, quindi, la *valutazione dei presìdi*, ossia l'analisi della robustezza ed efficacia dei controlli esistenti (ad esempio: backup e capacità di restore, segmentazione, patching, policy di crittografia, gestione delle identità, monitoraggio, procedure e audit sui fornitori) cui deve aggiungersi la determinazione del *rischio residuo* che sarà confrontata con il *risk appetite* (quantità e tipologia di rischio che si decide di accettare) perché indica dove l'esposizione eccede la tolleranza e richiede interventi prioritari.

L'intelligenza artificiale modifica il rischio ICT in due direzioni che coesistono e si alimentano. Da un lato, l'IA aumenta la capacità di osservazione e risposta[12], dall'altro lato, l'IA amplia la superficie d'attacco, la velocità di propagazione e le tipologie di fallimento.

Su queste basi, la gestione del rischio ICT richiede un processo di governo che renda misurabili impatto, priorità e rischio residuo, integrando monitoraggio continuo, gestione delle dipendenze di terze parti e presìdi specifici per l'IA. La figura seguente sintetizza questa sequenza operativa, mostrando come dalla mappatura e dall'analisi di impatto si arrivi a metriche, indicatori precoci e accountability, fino ai controlli dedicati ai sistemi AI.

Figura 1: *Processo di controllo e governo del rischio ICT*

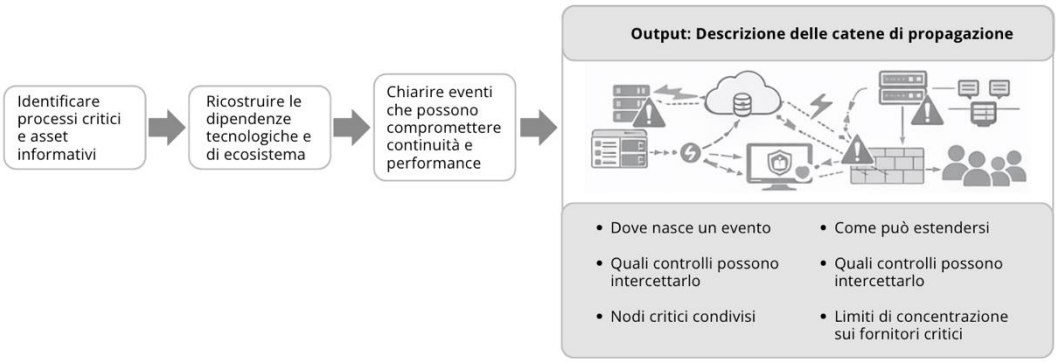
Fonte: Realizzazione dell'autore

3.1 Implementazione del monitoraggio del rischio ICT

La predisposizione di un modello di controllo e governo del rischio ICT richiede un percorso che trasformi vulnerabilità tecniche in variabili di governo strategico e renda misurabile la resilienza operativa. Il primo passaggio consiste nella costruzione di un'architettura enterprise-wide con cui l'impresa trasforma il rischio ICT in un oggetto di governo in modo da definire soglie operative coerenti con il risk appetite e di orientare: presìdi, escalation e allocazione delle risorse (cfr. figura seguente).

[12] Essa rende praticabile un monitoraggio continuo su volumi elevati di log, ticket e segnali esterni, abilita correlazione automatica tra eventi che altrimenti resterebbero dispersi, supporta anomaly detection su identità e traffico, migliora la triage degli alert, rafforza la prioritizzazione delle vulnerabilità combinando criticità tecnica e criticità di processo, consente analisi testuali su incident report per estrarre pattern ricorrenti e anticipatori

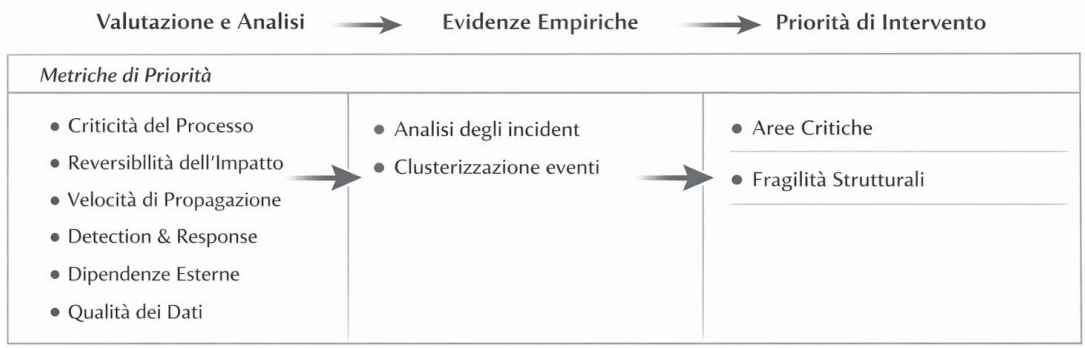
Figura 2: *Creazione dell'architettura enterprise wide*



Fonte: Realizzazione dell'autore

Il secondo passaggio consiste nella definizione di priorità e controllo, distinguendo rischio, efficacia dei presìdi e rischio residuo. Importante risulta l'utilizzo di una metrica che consenta di valutare esposizioni differenti secondo criteri omogenei che considerino diverse variabili. In questa fase, l'IA rafforza la qualità empirica del modello perché accelera l'estrazione di evidenze, pervenendo così ad una graduatoria delle priorità delle esposizioni e delle fragilità strutturali su cui indirizzare interventi e investimenti.

Figura 3: *Individuazione di priorità e sistemi di controllo*



Fonte: Realizzazione dell'autore

Il terzo passaggio è la *progettazione del sistema di monitoraggio continuo*, che richiede di affiancare KPI di servizio a KRI (Key Risk Indicators, indicatori precoci di rischio) utili per anticipare l'avvicinamento a soglie critiche. Un modello di governo efficace definisce per ciascun KRI: fonte del dato, soglia, frequenza di misura, regola di escalation e responsabile del rischio (risck owner). In ambito ICT, KRI tipici possono riguardare:

- identità e vantaggi: copertura MFA sugli account privilegiati, anomalie nei login, densità di privilegi elevati;

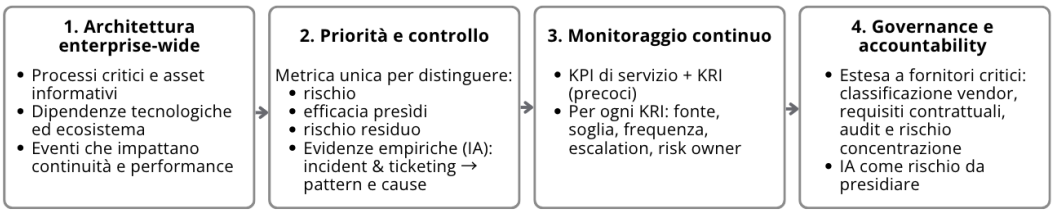
- superficie d'attacco: asset pubblici non inventariati, servizi esposti con configurazioni deboli;
- patching e vulnerabilità: latenza di patch su criticità elevate, backlog di CVE critiche su sistemi che supportano processi essenziali:
- stabilità del cambiamento: *change failure rate*, incidenti post-release:
- continuità e ripristino: successo verificato dei backup, esiti dei test di restore;
- tempi di *detection* e *containment* (alert ad alta severità non presi in carico entro SLA).

Il quarto snodo riguarda *governance e accountability* estese anche ai fornitori critici. Poiché una quota crescente di servizi è esternalizzata e organizzata su piattaforme, il modello richiede una classificazione dei vendor in base ai processi e ai servizi che supportano, requisiti minimi di sicurezza e continuità formalizzati a contratto e un ciclo di audit e monitoraggio che renda misurabili affidabilità e rischio di concentrazione. In chiave empirica, l'IA rafforza questo presidio rendendo più tempestiva l'evidenza: sintetizza report e attestazioni, segnala incidenti e vulnerabilità rilevanti per i fornitori in portafoglio, mette in relazione degradi degli SLA (Service Level Agreement, cioè l'insieme di livelli di servizio contrattualmente garantiti da un fornitore, o da una funzione interna, rispetto a un servizio ICT) con anomalie interne e ricostruisce le dipendenze tecniche più sensibili per individuare i punti in cui l'esposizione tende ad accumularsi.

Infine, l'IA va considerata anche come fonte autonoma di rischio. Quando entra nei processi, occorre garantirne governabilità e responsabilità nel tempo, rendendo esplicite le assunzioni e le condizioni di intervento qualora le prestazioni si riducano. Senza presìdi dedicati, l'aumento di velocità operativa può tradursi in fragilità, perché automatizza scelte e azioni, amplificando errori e dipendenze.

In sintesi, il monitoraggio del rischio ICT diventa efficace quando rende osservabili le catene causa-effetto che legano vulnerabilità, propagazione e impatto sui processi critici, traducendo tale evidenza in soglie, priorità e responsabilità di governo.

Figura 4: *Processo di implementazione e monitoraggio del rischio ICT*



Fonte: Realizzazione dell'autore

Caso aziendale (PMI) — Risk management in una impresa manifatturiera con e-commerce

Ipotizziamo l'azienda Meccatronica Salento S.r.l., PMI di manifattura leggera che integra la vendita di ricambi online su canali B2B e B2C. Queste le principali caratteristiche: 85 dipendenti; un fatturato annuo di € 18,2 mln; EBITDA dell'8,5% (circa € 1,55 mln); struttura dei ricavi bilanciata: il 65% deriva da vendite B2B con ordini ricorrenti, il 35% da e-commerce orientato a ricambi e componenti. I processi gestionali sono supportati da infrastruttura digitale come: ERP in cloud (SaaS), CRM, piattaforma e-commerce esterna con plugin, magazzino con barcode e pagamenti gestiti tramite PSP (Payment Service Provider).

Nel secondo trimestre l'impresa subisce tre eventi in sei settimane che rendono evidente la materialità del rischio ICT, perché gli effetti ricadono direttamente su consegne, incassi e fiducia commerciale. Il primo episodio è un downtime dell'ERP di 7 ore dovuto a un problema del provider SaaS: durante l'interruzione diventa impossibile emettere DDT e fatture e il picking rallenta. Il secondo episodio è un attacco phishing su un account con privilegi elevati, con tentativo di accesso alla console cloud e di acquisizione di dati clienti. Il terzo episodio è un degrado della piattaforma e-commerce, con aumento di latenza nel checkout e incremento degli errori di pagamento per quattro giorni, con conseguente calo del tasso di conversione.

La valutazione della materialità viene costruita traducendo gli eventi in impatti economici e operativi misurabili. Sul canale e-commerce, i dati medi sono 310 ordini al giorno con valore medio di € 165, pari a € 51.150 di ricavi giornalieri (310 × 165), con margine lordo medio del 32%.

Durante il downtime ERP, l'operatività si riduce del 60%, perché la gestione torna in parte manuale e solo per urgenze. Il ritardo accumulato è di 180 ordini. La stima del costo diretto considera il tempo extra di lavorazione: 180 ordini richiedono 12 minuti aggiuntivi ciascuno, pari a 2.160 minuti, cioè 36 ore. Con un costo orario medio di logistica e amministrazione pari a € 22/h, il costo diretto è € 792 (36 × 22). L'effetto più rilevante si concentra però sulla continuità B2B: 14 clienti ricevono consegne in ritardo e 2 clienti sospendono un ordine ricorrente mensile. Considerando un valore medio dell'ordine ricorrente di € 6.500/mese, la perdita potenziale è € 13.000/mese (2 × 6.500).

Il degrado e-commerce produce un effetto economico immediato e misurabile. Il *conversion rate* normale è 2,4% e durante il degrado scende a 1,7%. Con 9.000 visite al giorno, gli ordini attesi sarebbero 216 (9.000 × 2,4%), mentre quelli reali sono 153 (9.000 × 1,7%). La differenza è di 63 ordini persi al giorno. Con valore medio ordine di € 165, i ricavi persi al giorno sono € 10.395 (63 × 165). Su quattro giorni, i ricavi persi sono € 41.580. Applicando il margine lordo del 32%, il margine perso è € 13.306 (41.580 × 32%).

L'episodio di phishing non genera un data breach (violazione dei dati) accertato, ma comporta costi certi e rischio reputazionale elevato. L'impresa sostiene 18 ore di consulenza esterna per analisi forense a € 110/h, per un totale di € 1.980, e 14 ore di attività interne per reset credenziali e hardening, valorizzate a € 30/h, per € 420. Il costo complessivo è quindi € 2.400. Il board classifica l'evento come rischio materiale perché riguarda dati e fiducia, quindi potenzialmente la tenuta dei rapporti B2B.

In sintesi, nelle sei settimane considerate l'impatto immediato stimato è composto da € 3.192 di extra costi (evento A+B) e € 13.306 di margine perso sull'e commerce (evento C), per un totale di € 16.498, a cui si aggiunge un rischio di perdita ricavi futuri sul B2B stimato in € 13.000/mese per gli ordini ricorrenti sospesi. La conclusione manageriale è che il rischio ICT, in questa configurazione, entra nel perimetro del governo economico e commerciale, perché incide direttamente su continuità, margini e affidabilità percepita.

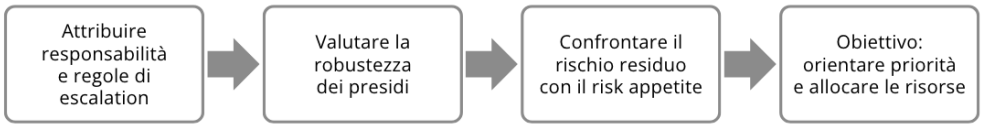
4. *Princìpi di governo del rischio: soglie, presìdi, decisioni*

Gli studi manageriali hanno dimostrato come la governance non tratti il rischio come una proprietà statistica delle alternative, ma come scostamento da obiettivi critici e come minaccia a soglie di performance, ciò al fine di definire priorità e comportamenti organizzativi (March e Shapira, 1987). L'individuazione di famiglie di rischio differenti, che richiedono approcci di governo diversi, ha condotto ad una classificazione dei rischi in prevenibili, strategici ed esterni, utile a rendere esplicito il legame tra natura dell'esposizione e architettura dei presìdi. Ne deriva uno spostamento dell'attenzione verso la coerenza tra tipo di rischio e procedure di gestione adottati.

Il risk management viene così inteso come un processo di governo che rende l'esposizione una variabile deliberata della decisione, collegando obiettivi, soglie e presìdi in un ciclo continuo di valutazione e revisione.

La coerenza tra natura del rischio e architettura di gestione diventa un criterio centrale: rischi differenti richiedono presìdi differenti, una classificazione adeguata evita che l'organizzazione applichi risposte standard a esposizioni eterogenee. In chiave ERM (Enterprise Risk Management), il risk management assume una logica enterprise-wide: integra le esposizioni in una vista trasversale e si innesta nei processi che generano la scelta, collegando strategia, obiettivi, performance e reporting. L'efficacia dipende dalla qualità di questo innesto e dalla coerenza con il contesto competitivo e organizzativo.

Figura 5: *Ciclo escalation, valutazione e risk appetite*



Fonte: Realizzazione dell'autore

La formalizzazione di un modello di risk management richiede una struttura che trasformi il rischio da etichetta descrittiva a variabile governabile, cioè collegata a confini, responsabilità, soglie e meccanismi di revisione.

Il punto di partenza è il perimetro: senza una definizione dei confini, l'esposizione resta dispersa e non confrontabile. In questa fase, l'impresa identifica i rischi rilevanti lungo l'intera catena di creazione del valore, includendo le dipendenze tecnologiche e di servizio (cloud provider, piattaforme, software di terze parti, outsourcer, API). Operativamente, ciò implica la definizione di un elenco dei servizi e degli asset critici e di una mappa delle dipendenze, perché il rischio non si manifesta solo come evento ma come possibilità di propagazione attraverso interfacce e componenti condivisi.

Definito il perimetro, diventa centrale la *materialità*, cioè il criterio con cui un rischio diventa "strategico". Il rischio assume rilevanza manageriale quando è in grado di incidere su continuità operativa e quando la sua dinamica temporale riduce la reversibilità delle scelte. In pratica, un rischio è materiale quando può interrompere o degradare funzioni essenziali, oppure quando può distorcere la qualità del dato e, di conseguenza, la qualità della decisione. In questa fase, l'uso di strumenti di *process mining* consente di quantificare l'impatto di un degrado operativo su tempi di ciclo, colli di bottiglia e performance, riducendo la distanza tra rischio "tecnico" e danno "di business".

> Il process mining è una classe di strumenti che ricostruisce i processi reali osservando le tracce che i sistemi informativi lasciano nelle attività quotidiane. Invece di partire da flowchart o interviste, il process mining parte dai dati e rende visibili sequenze operative, varianti, tempi di attraversamento, attese e ricorsività (rework), cioè gli elementi che determinano sia la performance sia le aree di fragilità.
> Dal punto di vista tecnico, il cuore è l'event log: un insieme di registrazioni in cui ogni riga descrive un evento associato a uno specifico "caso" (un ordine, una pratica, un ticket, un reso). Ogni evento contiene almeno un identificativo del caso, il nome dell'attività e un timestamp; spesso sono disponibili anche informazioni su chi o cosa ha eseguito l'azione, su canale, priorità, categoria, costo o esito. Un tool come Celonis si collega ai sistemi sorgente (ERP, CRM, ITSM, piattaforme di e-commerce, ecc.), estrae questi eventi e li organizza in modo coerente, così da poter ricostruire il processo come rete di passaggi osservati e non come modello teorico.
> Una volta costruito l'event log, lo strumento applica algoritmi di discovery per ricostruire il "processo as-is" e calcolare le metriche che contano: quanto dura il ciclo end-to-end, dove si accumulano attese, quante varianti esistono davvero, quali passaggi si ripetono e con quale frequenza. A questo si affianca, quando necessario, la verifica di conformità: il processo reale viene confrontato con un processo atteso (uno standard interno, una policy, una sequenza desiderata) per evidenziare deviazioni e punti in cui la disciplina operativa si indebolisce. Un ulteriore livello è l'analisi dei driver: segmentando casi e varianti per caratteristiche (tipologia di cliente, canale, fornitore, classe prodotto, priorità del ticket), il process mining permette di isolare le condizioni che spiegano ritardi, errori, rework o fallimenti.
> La ragione per cui questi strumenti sono rilevanti nel risk management è che consentono di quantificare la materialità e di collegare rischio e impatto in modo empirico. Se un incidente ICT degrada un servizio, il process mining mostra come quel degrado si traduce in accumulo di tempi, raddoppio di passaggi, aumento di eccezioni o blocchi su specifiche tratte del processo. In questo modo il rischio non resta "tecnico" e la governance non è costretta a scegliere sulla base di percezioni: si rende misurabile la propagazione dell'effetto sui processi critici e diventa più naturale definire soglie, priorità e indicatori precoci coerenti con continuità operativa e performance.

La terza componente riguarda le soglie, cioè la traduzione del risk appetite in tolleranze operative misurabili e in trigger di escalation. Il risk appetite, in chiave applicativa, consiste in un set di limiti entro cui l'impresa accetta di operare: indisponibilità massima per servizio, obiettivi di ripristino (RTO Recovery Time Objective e RPO: Recovery Point Objective/RPO), livelli minimi di controllo su identità e privilegi, vincoli di concentrazione su fornitori critici. Il punto di governo

è che tali soglie devono essere collegate a decisioni: superato un certo limite, il monitoraggio lascia spazio alla decisione. Per rendere questo meccanismo robusto, il modello deve prevedere escalation differenziate (warning e critical), ownership esplicita e tracciabilità delle assunzioni.

A valle delle soglie si collocano i presìdi, che sono la parte più spesso fraintesa perché tende a ridursi a un elenco di controlli. In realtà, i presìdi sono efficaci solo se coerenti con la natura dell'esposizione:

- controlli e standard per i rischi prevenibili;
- segmentazione, backup verificati e architetture resilienti per i rischi di indisponibilità;
- piani di risposta e capacità di ripristino per contenere l'impatto e ridurre la durata dell'interruzione;
- audit e requisiti minimi per le terze parti, quando la vulnerabilità entra nel perimetro attraverso fornitori e piattaforme.

Applicazioni operative di Tool chiave per rendere misurabili i presìdi di sicurezza

L'uso combinato di piattaforme di monitoraggio, risposta e gestione delle vulnerabilità consente di trasformare i presìdi da adempimenti "documentali" a capacità operative verificabili, perché rende tracciabili rilevazione, contenimento e riduzione del rischio residuo.

SIEM – Microsoft Sentinel / Splunk

Raccolgono e normalizzano log e telemetrie (cloud, rete, identità, endpoint, applicazioni) e applicano regole di correlazione e analisi per individuare sequenze anomale e pattern di attacco. Il valore sta nella capacità di unificare segnali dispersi e produrre alert contestualizzati, riducendo rumore e falsi positivi tramite enrichment e scoring.

SOAR – Cortex XSOAR

Orchestrano la risposta attraverso playbook eseguibili: arricchimento automatico dell'alert (threat intel e contesto), attivazione di azioni di contenimento (isolamento, blocco credenziali, quarantena), apertura e gestione ticket, raccolta evidenze. Il funzionamento è basato su workflow parametrizzati e integrazioni via API con gli strumenti di security e ITSM, con l'obiettivo di comprimere detection-to-response e standardizzare la gestione degli incidenti.

EDR/XDR – Microsoft Defender for Endpoint / CrowdStrike

Forniscono telemetria continua dagli endpoint e capacità di rilevazione e risposta: individuano comportamenti sospetti, tracciano catene di esecuzione e lateral movement, permettono azioni immediate (isolare host, terminare processi, bloccare indicatori). Le funzionalità XDR estendono la correlazione oltre l'endpoint, integrando segnali di identità, email e cloud per ricostruire la "kill chain" e accelerare l'investigazione.

Vulnerability Management – Tenable / Rapid7

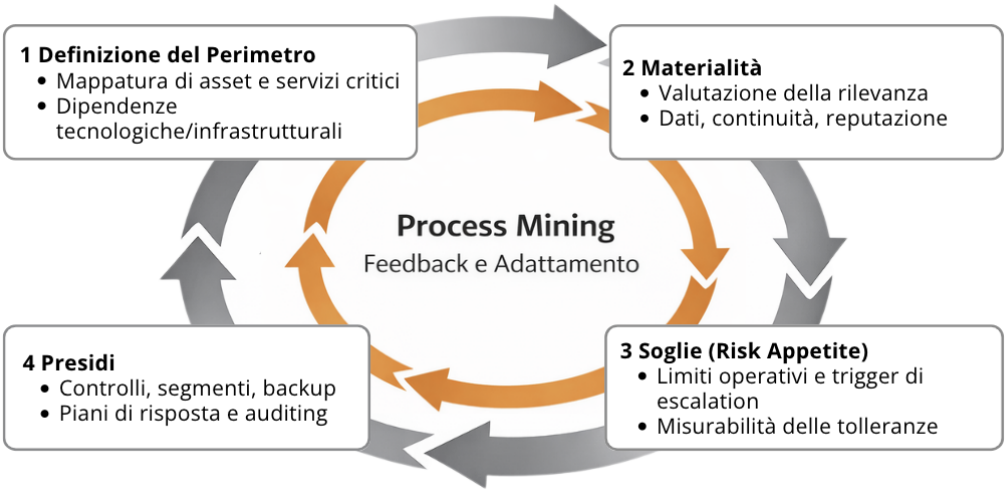
Identificano vulnerabilità e misconfigurations su asset e servizi, stimano la criticità e supportano la prioritizzazione degli interventi. Operano tramite scanning (rete, agent, cloud) e scoring che combina severità tecnica, esposizione e contesto; l'obiettivo è guidare remediation e patching verso ciò che riduce davvero il rischio residuo sui processi critici, non verso ciò che aumenta solo il volume di attività.

Insieme, questi tool sostengono una logica unica: rendere misurabili la postura, i tempi di risposta e l'efficacia dei presìdi, così che la governance possa

intervenire su priorità e allocazione delle risorse in modo coerente con soglie e rischio residuo.

Per evitare che il modello resti episodico, occorre avere un sistema di indicatori che colleghi performance e vulnerabilità. In questa prospettiva, i KPI misurano esiti e livelli di servizio, mentre i KRI segnalano l'avvicinamento a soglie critiche e rendono possibile intervenire prima che l'evento si manifesti. È qui che l'IA produce un salto qualitativo perché rende trattabile il monitoraggio continuo su volumi elevati e su sorgenti eterogenee. L'*anomaly detection* su identità e traffico, la correlazione automatica di eventi distribuiti, la classificazione e prioritizzazione degli alert e l'analisi testuale di ticket riducono il rumore e aumentano la qualità del segnale.

Figura 6: *Ciclo di formalizzazione del risk management*



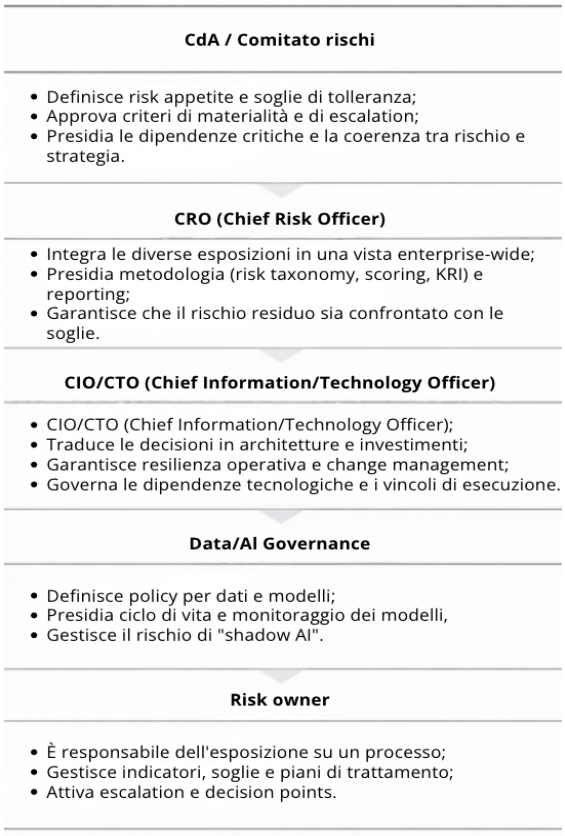
Fonte: Realizzazione dell'autore

Infine, un modello formalizzato richiede un feedback strutturato: revisione periodica delle assunzioni, aggiornamento degli scenari, verifica dell'efficacia dei presìdi, ritaratura di soglie e indicatori. Questo ciclo è la parte che rende il modello "strategico", perché sposta la gestione del rischio dalla reazione alla progettazione: ciò che viene appreso dagli incidenti deve modificare playbook, controlli e architetture. Se l'impresa utilizza modelli di IA in produzione, il feedback include anche il monitoraggio di drift e degradazione, con meccanismi di rollback e responsabilità chiare, perché la componente algoritmica introduce un profilo di rischio che va governato con la stessa disciplina applicata a processi e infrastrutture. In questo modo, il risk management non si limita a registrare l'esposizione, ma istituzionalizza un linguaggio comune e un ciclo decisionale che mantiene allineati rischio, strategia e capacità operativa nel tempo.

5. *Risk Management: architettura e implicazioni manageriali*

Un modello di risk management diventa realmente operativo quando si traduce in un'architettura stabile di ruoli, processi e *deliverable* che rende il rischio una variabile deliberata della decisione, non un'informazione accessoria. Diventa fondamentale giungere ad una capacità di governo che mantenga coerenti strategia, tolleranze e presìdi, soprattutto in contesti in cui la velocità del cambiamento rende fragile qualsiasi impostazione puramente ex post. L'introduzione dell'IA accentua questa esigenza: aumenta la capacità di osservazione e risposta, ma introduce anche nuove vulnerabilità e nuove dipendenze che richiedono accountability, tracciabilità e meccanismi di revisione.

Figura 7: *Ruoli e responsabilità nella governance del rischio enterprise-wide*



Fonte: Realizzazione dell'autore

Il modello di risk management richiede un'architettura di responsabilità chiara, capace di collegare soglie, decisioni e presìdi operativi. La governance definisce criteri e tolleranze, le funzioni di risk e technology le traducono in metodo e in architetture esecutive, mentre i responsabili di processo garantiscono monitoraggio ed escalation. In questo modo, il rischio residuo diventa misurabile e governabile, con priorità e investimenti coerenti con la strategia.

In termini applicativi, la distinzione chiave riguarda chi definisce le soglie e chi gestisce la variabilità entro quelle soglie. L'IA non sostituisce questa architettura: la rende più esigente, perché aumenta la velocità con cui segnali e incidenti possono emergere e propagarsi.

Il risk management diventa efficace quando è innestato nei passaggi che generano scelte e impegni di risorse.

Figura 8: *Attività necessarie per attivare il risk management*

Fonte: Realizzazione dell'autore

Il *primo passaggio è il budgeting* in cui assume rilevanza il CAPEX (*Capital Expenditures*, indica gli investimenti in conto capitale) che analizza il rischio nella selezione degli investimenti perché rende esplicito quali opzioni richiedono presìdi, ridondanze, capacità di ripristino o riduzione di dipendenze critiche. La priorità, di conseguenza, deriva dal rapporto tra criticità del processo, rischio residuo e soglie deliberate, così che l'allocazione delle risorse rimanga coerente nel tempo.

Un *secondo snodo riguarda le iniziative di IA*, che richiedono un percorso di "gate" minimo per evitare che la messa in produzione preceda le evidenze necessarie. In pratica, la governance deve chiarire quali casi ricadono in area "alto rischio" e quale set di verifiche rende legittimo il go-live.

MLOps e controllo del passaggio in produzione

Le MLOps (*Machine Learning Operations*) sono l'insieme di pratiche, ruoli e strumenti che rendono sviluppo, rilascio e gestione in esercizio dei modelli di *machine learning* tracciabili, ripetibili e governabili. La misurabilità del passaggio in produzione di iniziative di IA dipende dall'adozione di pratiche MLOps che rendano il ciclo di vita del modello tracciabile, ripetibile e controllabile. L'obiettivo è poter rispondere in modo documentabile a tre domande: *quale versione del modello è in esercizio, su quali dati e test è stata approvata, come si interviene se le prestazioni degradano*.

Dal punto di vista operativo, le pratiche chiave riguardano:

- Versioning di modello, dataset e feature: ogni rilascio deve essere identificabile e ricostruibile, evitando che cambiamenti "invisibili" (dati, preprocessing, feature store) alterino i risultati senza controllo.
- Tracciabilità dei test: oltre alle metriche di accuracy, serve evidenza dei test rilevanti per il contesto d'uso (robustezza, stabilità su segmenti critici, regressioni rispetto alla versione precedente, controlli su leakage).
- Audit trail: registrazione di chi ha modificato cosa, quando e con quale razionale, includendo approvazioni e criteri di go/no-go, in modo coerente con governance e accountability.
- Rollback e fallback: procedure per tornare a una versione precedente o a una modalità alternativa di funzionamento quando emergono drift, anomalie o incidenti, riducendo il tempo di esposizione.

Strumenti come MLflow supportano questi requisiti perché consentono di tracciare esperimenti, parametrizzazioni, metriche e artefatti del modello, mantenendo uno storico delle versioni e delle evidenze a supporto della validazione. Piattaforme come Azure ML, Vertex AI e SageMaker estendono la disciplina a livello di pipeline e messa in produzione: orchestrano training e deployment, gestiscono registri dei modelli, automatizzano controlli di qualità e abilitano un rilascio controllato (ad esempio con validazioni e passaggi di approvazione), rendendo ripetibile il processo e riducendo l'arbitrarietà del "go-live".

In sintesi, l'MLOps trasforma un rilascio di IA da evento tecnico a passaggio governato: ciò che viene messo in produzione è definito, verificabile e reversibile.

Il *terzo snodo è la revisione delle assunzioni critiche*: dipendenze da piattaforme, qualità dei dati, capacità di risposta, stabilità di fornitori e modelli non possono restare implicite. Devono diventare oggetti di governo, collegati a soglie e indicatori precoci che attivano punti di decisione quando cambiano le condizioni di validità; qui l'IA può supportare l'early warning attraverso correlazione di segnali deboli, *anomaly detection* su serie temporali operative e analisi testuale su ticket e *incident report*.

Deliverable stabili per il modello di governo del rischio

Per rendere operativo e verificabile il modello di governo del rischio servono deliverable stabili, perché sono l'infrastruttura che consente di misurare l'allineamento tra esposizione, presìdi, soglie e priorità decisionali. La logica è semplice: ciò che non è rappresentato in artefatti ripetibili tende a restare implicito, quindi non governabile.

Una dashboard integrata KPI+KRI fornisce la vista utile al processo decisionale. I KPI misurano continuità e livelli di servizio; i KRI anticipano l'avvicinamento a soglie critiche su identità e privilegi, patch latency, esposizione degli asset, esiti dei test di restore e alert non presi in carico. Dal punto di vista tecnico-operativo, la qualità della dashboard dipende da tre scelte: (i) normalizzazione e deduplicazione delle fonti (log e telemetrie, ticketing, posture cloud), (ii) definizione di soglie e regole di escalation direttamente nel modello dati, (iii) tracciabilità della "lineage" degli indicatori, cioè la possibilità di risalire dal numero in dashboard alla fonte e all'evento che lo genera. Power BI o Tableau possono ospitare la sintesi, ma la credibilità della vista dipende dall'integrazione con fonti operative come SIEM, ITSM/ticketing e strumenti di cloud posture, oltre alla gestione di refresh, latenza e qualità del dato.

Quando l'IA entra nei processi, serve un reporting specifico sugli incidenti IA, perché il fallimento non coincide solo con indisponibilità o attacco: può manifestarsi come drift, errori sistematici, leakage, misuse o failure di pipeline. Il reporting deve includere condizioni di attivazione, impatto, contenimento, root cause e correzioni, con aggiornamento coerente di soglie e modello.

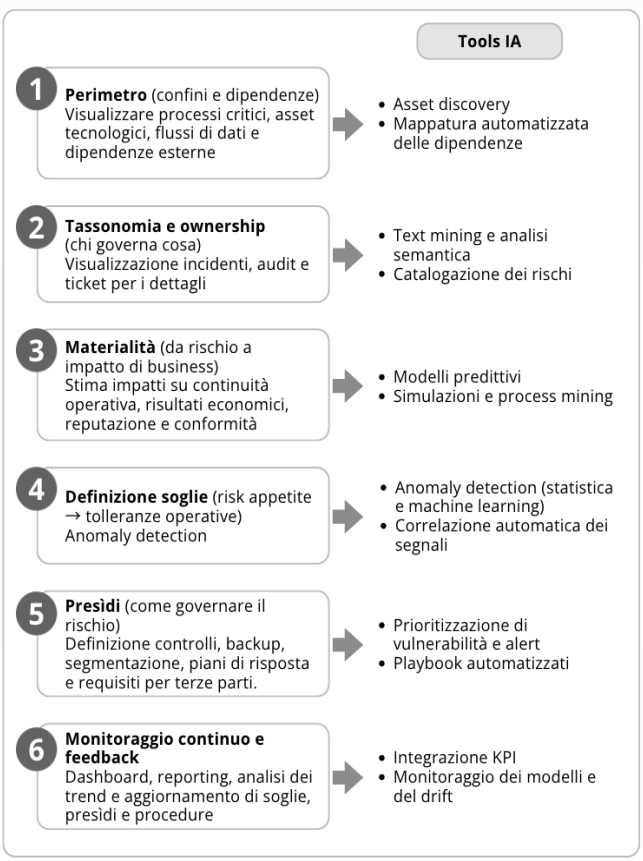
Nel loro insieme, questi deliverable rendono verificabile il modello perché convertono il governo del rischio in un sistema osservabile: soglie esplicite, indicatori affidabili, assunzioni tracciate, risposta eseguibile e apprendimento incorporato.

Il risk management funziona, dunque, come infrastruttura di decisione e diventa rilevante soprattutto in condizioni di complessità: chiarisce dove la variabilità è accettabile, dove scattano soglie e quale forma assume la responsabilità quando le condizioni cambiano. Se i processi incorporano il rischio prima della decisione e i deliverable rendono visibili soglie e presìdi, la governance può mantenere l'equilibrio tra disciplina e capacità di competere. In questo impianto, l'IA rafforza osservazione e reazione e rende più rapida la verifica empirica delle fragilità; fuori dall'impianto, accelera operazioni e dipendenze e rende più probabile che l'instabilità emerga prima che l'organizzazione abbia modo di correggere.

6. *Dal modello al piano di risk management*

La realizzazione di un processo di risk management richiede una sequenza strutturata di fasi (in parte già viste nelle pagine precedenti e qui riproposte per sintesi esplicativa) tra loro interdipendenti, attraverso le quali l'esposizione al rischio viene progressivamente resa osservabile, valutabile e governabile. L'intelligenza artificiale interviene lungo l'intero processo come supporto alla capacità dell'impresa di gestire complessità informativa, interdipendenze operative e dinamiche temporali, senza assumere un ruolo sostitutivo della responsabilità decisionale.

Figura 9: *Processo di Risk Management AI-driven*



Fonte: Realizzazione dell'autore

La prima fase riguarda la *definizione del perimetro*, poiché ogni attività di governo del rischio presuppone confini chiari entro cui l'esposizione possa essere rilevata e confrontata. In questa fase, l'impresa identifica processi critici, asset tecnologici e informativi, flussi di dati e dipendenze esterne che sostengono la creazione di valore. Tool di IA e *analytics* permettono di collegare segnali operativi a impatti economici: ad esempio, analisi su serie storiche per stimare costo del fermo impianto, oppure *process mining* per misurare dove il degrado ICT crea colli di bottiglia. Il risultato è una rappresentazione dinamica del perimetro operativo, che riduce asimmetrie informative e rende esplicite le aree di possibile propagazione del rischio.

Il processo prosegue poi con la *tassonomia e l'assegnazione delle responsabilità*, necessarie per rendere il rischio interpretabile e governabile. I rischi vengono classificati secondo categorie coerenti con la loro natura e assegnati a specifici risk owner. In questa fase, l'IA contribuisce a:

- analizzare incidenti, audit e ticket storici tramite tecniche di text mining;
- uniformare il linguaggio utilizzato per descrivere eventi e vulnerabilità;

- supportare la costruzione di un registro dei rischi coerente nel tempo.

La fase successiva è la *valutazione della materialità*, che serve a separare le esposizioni che possono alterare continuità operativa, risultati economici, reputazione e conformità da quelle che restano marginali. Qui l'IA consente di passare da una stima qualitativa ad una quantificazione coerente con i processi e con i dati disponibili: integra segnali interni ed esterni (log operativi, incidenti, audit, ticket, dati di filiera, indicatori di mercato), costruisce serie storiche pulite e comparabili, e rende replicabile il passaggio da "evento" a "impatto".

I modelli predittivi supportano la stima delle conseguenze attese di specifici eventi, distinguendo impatti diretti e indiretti: perdita di margine, ritardi, scarti, penali, aumento del costo del servizio, degrado della qualità percepita. Le simulazioni di scenario, come le tecniche Monte Carlo, rendono osservabile la variabilità degli esiti e la loro probabilità, così da valutare materialità non solo per valore medio, ma anche per coda di rischio e condizioni di stress. Gli strumenti di *process mining* e *task mining* collegano gli eventi di rischio ai flussi reali di lavoro, individuando punti di fragilità e propagazione dell'impatto lungo i processi, con evidenza su colli di bottiglia, rework, tempi di attraversamento e dipendenze tra funzioni e terze parti. Ne deriva una scala di priorità costruita su evidenze empiriche e tracciabili, utile per confrontare rischi eterogenei con una metrica comune e per motivare scelte di trattamento, investimenti e soglie di escalation.

La fase successiva consiste nella *definizione delle soglie*, che traduce il *risk appetite* in tolleranze operative misurabili. Le soglie stabiliscono quando l'esposizione rientra nei limiti accettabili e quando richiede una presa in carico decisionale. Qui l'IA interviene attraverso:

- sistemi di *anomaly detection* che intercettano variazioni significative rispetto ai livelli attesi;
- correlazione automatica di segnali deboli provenienti da fonti eterogenee;
- monitoraggio continuo degli indicatori associati ai processi critici.

Il superamento delle soglie avvia la *progettazione e l'attivazione dei presìdi*, intesi come configurazioni coerenti di regole, procedure e strumenti, calibrate sulla natura del rischio e sul livello di esposizione accettato. L'IA interviene soprattutto nel rendere più selettiva e tempestiva la risposta operativa, perché permette di trasformare molti segnali disomogenei in una sequenza di azioni ordinata, verificabile e ripetibile. In concreto:

- piattaforme come *Microsoft Sentinel* o *Splunk* raccolgono eventi e log provenienti da sistemi diversi e, grazie a funzioni di analisi e correlazione, aiutano a distinguere i segnali davvero rilevanti da quelli di routine;
- strumenti di automazione della risposta come *Cortex XSOAR* eseguono procedure predefinite quando si supera una soglia o si verifica un evento critico, ad esempio aprendo automaticamente un ticket, avvisando i responsabili, raccogliendo evidenze, applicando misure immediate di contenimento;

- componenti basati su *LLM*, collegati alla documentazione interna tramite sistemi di ricerca e consultazione guidata, supportano il triage sintetizzando ticket e segnalazioni, raggruppando casi simili e restituendo una traccia operativa coerente con i runbook aziendali.

Infine, l'IA abilita l'orchestrazione della risposta tramite playbook eseguibili e tracciabili, che coordinano attività ricorrenti come raccolta evidenze, isolamento di asset, reset di credenziali, apertura e aggiornamento di ticket, comunicazioni interne e, quando previsto, attivazione del vendor.

Il presidio resta una scelta manageriale perché implica trade off tra costo, efficacia e sostenibilità nel tempo; l'IA ne aumenta l'efficienza operativa e la ripetibilità, rendendo più stabile il passaggio da segnale ad intervento e più misurabile la riduzione del rischio residuo.

Il processo si completa con il monitoraggio continuo e il feedback strutturato, che rendono il risk management un sistema capace di aggiornarsi nel tempo anche attraverso l'impiego dell'I.A., come:

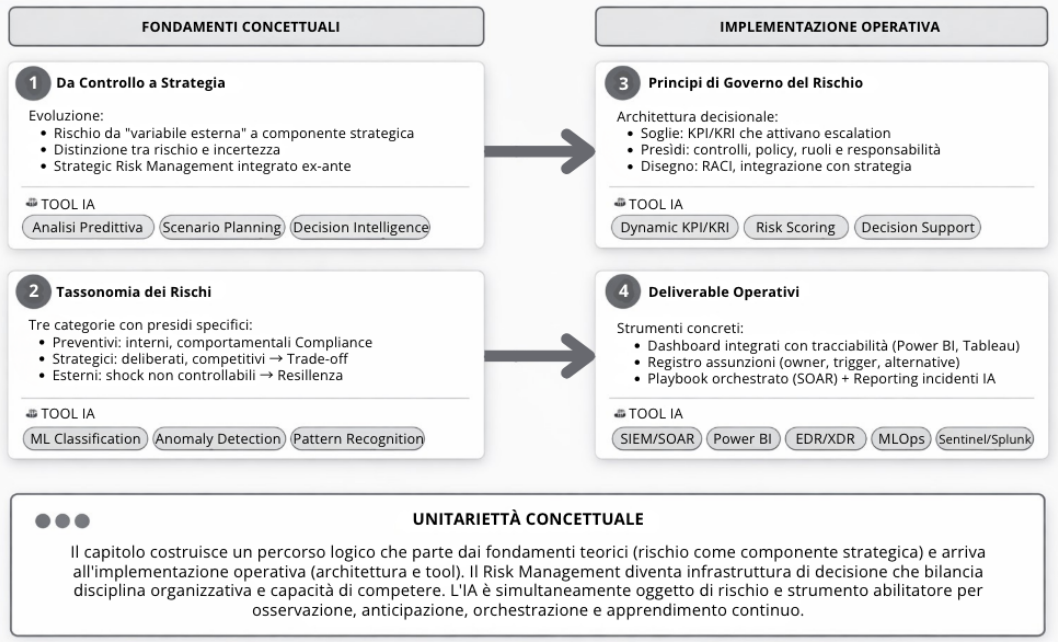
- strumenti di dashboard e reporting come *Power BI* o *Tableau* consentono di integrare *KPI e KRI* in viste coerenti, aggiornate e leggibili, collegando indicatori operativi, segnali di rischio e soglie di escalation;
- piattaforme di analisi e monitoraggio come *Splunk* o *Microsoft Sentinel* aiutano a sintetizzare trend, evidenziare ricorrenze e portare in superficie pattern che, su base manuale, resterebbero frammentati tra log, ticket e report;
- soluzioni basate su *LLM* possono supportare la fase di apprendimento, sintetizzando incidenti, raggruppando casi simili, ricostruendo le cause ricorrenti e producendo una traccia utilizzabile per aggiornare procedure, presìdi e soglie.

Quando l'impresa utilizza modelli di IA nei propri processi, il feedback include anche il controllo della componente algoritmica. Strumenti di gestione del ciclo di vita dei modelli come *MLflow*, *Azure Machine Learning* o equivalenti permettono di monitorare nel tempo le prestazioni, rilevare derive, gestire versioni e, quando necessario, ripristinare una versione precedente. In questo modo, il rischio legato ai modelli viene governato con la stessa logica applicata ai processi: indicatori, soglie, responsabilità e meccanismi di revisione.

Nel loro insieme, queste fasi delineano un processo di risk management che integra osservazione, decisione e apprendimento in modo continuo. L'intelligenza artificiale aumenta la capacità di osservazione e la tempestività delle risposte, rendendo più verificabile la gestione del rischio residuo, mentre la governabilità del sistema dipende dalla chiarezza delle soglie, dalla coerenza dei presìdi e dalla stabilità dei meccanismi di feedback.

Implicazioni gestionali
Quanto esposto in questo capitolo può intendersi come un percorso logico che collega princìpi teorici ed operatività, mostrando come il risk management diventi un'infrastruttura di decisione e non un esercizio di controllo ex post.
La sequenza parte dall'evoluzione concettuale: il rischio viene trattato come scostamento da obiettivi critici e come minaccia a soglie di performance, quindi come variabile che orienta priorità e comportamenti organizzativi.

Figura 10: *Schema logico risk management*



Fonte: Realizzazione dell'autore

In questa prospettiva, assume rilievo la distinzione tra rischio e incertezza: quando le probabilità sono stimabili, l'impresa può ragionare su distribuzioni e impatti attesi; quando prevale l'incertezza, la qualità della decisione dipende dalla robustezza delle architetture decisionali, dalla gestione delle assunzioni e dalla capacità di adattamento. Sul piano gestionale, la prima ricaduta di quanto esposto consiste nella distinzione tra rischio e incertezza e nel passaggio ad una logica SRM/ERM.
SRM – Strategic Risk Management
Approccio che tratta il rischio come parte della scelta strategica focalizzando l'attenzione sui rischi legati a posizionamento, investimenti, tecnologie, mercati e dipendenze dell'ecosistema valutandone anche eventuali opportunità.
ERM – Enterprise Risk Management
È l'approccio che istituzionalizza il governo del rischio nell'organizzazione poiché integra rischi diversi in una visione d'insieme, definisce ruoli e responsabilità, metodologie comuni con l'obiettivo di evitare silos e rendere confrontabile il rischio residuo rispetto alle soglie deliberate.
SRM definisce *quali* rischi strategici devono entrare nella decisione e *come* governarli in relazione a obiettivi e scelte competitive. ERM fornisce la struttura organizzativa e informativa per farlo in modo sistematico, continuo e verificabile.
Su questo impianto si innesta la tassonomia, che chiarisce che "rischio" non è una categoria unica. La distinzione tra rischi prevenibili, strategici ed esterni

rende esplicito il legame tra natura dell'esposizione e modalità di gestione appropriate. La classificazione ha una sua utilità operativa: evita, infatti, che l'organizzazione applichi risposte standard a esposizioni eterogenee e consente di collegare ciascuna famiglia di rischio a pratiche coerenti, riducendo rigidità decisionali, tolleranze improprie e illusioni di controllabilità.
Dal piano concettuale si passa ai princìpi di governo, che traducono il rischio in una variabile deliberata della decisione. Il punto di snodo sono le soglie: KPI e KRI non servono solo a misurare, ma a rendere esplicito quando l'organizzazione deve attivare *escalation* e *decision points*. Le soglie delimitano il campo di operatività accettabile e collegano rischio e performance a responsabilità definite. In parallelo, il governo richiede presìdi coerenti con l'esposizione e una disciplina di accountability che chiarisca ruoli, deleghe e responsabilità, assicurando l'innesto nei processi che generano la scelta.
In questo schema, l'IA assume una doppia valenza. Da un lato rafforza la qualità empirica del governo: rende trattabile il monitoraggio continuo su volumi elevati di segnali, accelera l'estrazione di evidenze, supporta correlazione di eventi, prioritizzazione e apprendimento post-incidente. Dall'altro lato, l'IA introduce un profilo di rischio proprio, che richiede tracciabilità, controllo del ciclo di vita e responsabilità chiare, perché la velocità operativa può trasformarsi in instabilità quando automatizza decisioni e azioni senza garanzie di qualità nel tempo.
L'esposizione della gestione del rischio ICT ci illustra come passare dalla descrizione (riservatezza, integrità, disponibilità) ad una lettura causa-effetto, distinguendo profilo applicativo, infrastrutturale e cyber. Nella realtà questo serve perché incidenti analoghi producono impatti simili, ma possono nascere da cause diverse e, quindi, richiedono interventi diversi. La mappa delle dipendenze e delle catene di propagazione consente di identificare i punti di guasto condivisi: dove un'anomalia locale può estendersi lungo connessioni operative e dipendenze fino a diventare un problema enterprise-wide.
L'esposizione sin qui condotta fa emergere altresì il concetto di *risk appetite* traducendolo in tolleranze misurabili (indisponibilità massima per processo, RTO/RPO, vincoli di perdita dati, requisiti minimi su identità/privilegi, limiti di concentrazione su fornitori critici). La ricaduta manageriale è evidente se si considera come le soglie diventino trigger che spostano l'organizzazione dal monitoraggio alla decisione, con regole di escalation e ownership esplicita.
L'IA entra in questo processo come acceleratore "empirico": riduce i costi di estrazione delle evidenze ed aumenta la qualità del segnale, soprattutto quando le fonti sono molte e frammentate (log, ticket, audit, report fornitori, telemetrie cloud). Diventa fondamentale per la gestione rendere verificabili perimetro, priorità e rischio residuo, quindi:

- asset discovery e CSPM per rendere affidabile l'inventario reale e la postura cloud;
- analisi di incident e ticketing (anche con NLP) per individuare ricorrenze, failure mode e pattern che anticipano degradazioni;
- correlazione eventi e orchestrazione della risposta (SIEM/SOAR) per comprimere detection-to-response e standardizzare i playbook;
- pratiche MLOps (versioning, audit trail, rollback) quando l'IA è parte del processo e deve restare governabile nel tempo.

Da questo impianto emerge un linguaggio di governo che, con riferimento ai rischi, collega perimetro e dipendenze, criteri di materialità, soglie che attivano decisioni, meccanismi di gestione verificabili, indicatori precoci e feedback strutturato. In questo assetto, l'IA agisce come moltiplicatore di osservabilità ed evidenza, perché riduce il rumore informativo ed accelera la trasformazione dei segnali in priorità e delle priorità in scelte tracciabili, mantenendo la responsabilità decisionale in capo alla governance.

BIBLIOGRAFIA

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of Management, 43*(1), 39–58.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review, 49*(1), 56–74.

Gawer, A. (2021). Digital platforms' boundaries: The interplay of firm scope, platform sides, and digital interfaces. *Long Range Planning, 54*(5), Article 102045.

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301–327.

Hardy, C. O. (1931). *Risk and risk-bearing* (Rev. ed.). University of Chicago Press.

Horneber, D., & Laumer, S. (2023). Algorithmic accountability. *Business & Information Systems Engineering, 65*(6), 723–730.

International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60.

Knight, F. H. (1921). *Risk, uncertainty, and profit*. Houghton Mifflin.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404–1418.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, recante norme armonizzate sull'intelligenza artificiale (Artificial Intelligence Act). (2024). *Gazzetta ufficiale dell'Unione europea, L 2024/1689*.

Tapinos, E., Kamarulzaman, N. H., & Aouad, G. (2019). Rethinking strategic risk management: New trends and directions for future research. *Business Horizons, 62*(6), 733–743.