Rischi non finanziari: dalla frammentazione all'integrazione

Third Party Risk Management, un caso reale di integrazione tra rischi

Roberta Ranaldi, Intesa Sanpaolo

10 Giugno 2026

Agenda

1. Dal rischio operativo alla gestione integrata dei rischi non finanziari

2. Metodologia, processi e soluzioni tecnologiche per il TPRM

3. Principali implicazioni derivanti da una gestione integrata del rischio derivante da terzi

L'evoluzione normativa alla base dell'attuale gestione dei rischi non finanziari

Dall'introduzione del **rischio operativo** con Basilea II alle più recenti normative sulla **resilienza**, la gestione dei rischi non finanziari si è evoluta fino a diventare un **elemento centrale per la solidità delle banche**, con un'attenzione crescente alla resilienza tanto del business quanto delle infrastrutture.

Rischio Operativo

- **Basilea II** (2004) introduce il **rischio operativo** come **categoria residuale** rispetto ai rischi finanziari (i.e. mercato, liquidità e credito), attribuendogli una rilevanza autonoma nel framework regolamentare.
- **Il framework si focalizza** in particolare su
  - **Perdite operative**
  - **Misurazione e gestione del capitale**
  - **Attività di controllo**

Gestione dei rischi non finanziari

- L'attività di rilevazione dei rischi si è progressivamente evoluta verso un **approccio di governance olistica del rischio,** in risposta all'introduzione di **regolamentazioni e linee guida tematiche**, quali:
  - **GDPR**
  - **NIS**
  - **DORA**
  - **EBA Guidelines** (e.g., Outsourcing, Fraud Reporting, SREP, ICT & Security, Major Incients)
- Si **amplia il perimetro dei rischi**, includendo anche le componenti reputazionale e strategica, con un progressivo **spostamento del focus verso la resilienza**.

Dalle normative tematiche alla definizione di una tassonomia comune dei rischi non finanziari

Il regolatore introduce una lettura dei rischi non finanziari basata su una tassonomia comune, che ne evidenzia la **natura trasversale** e favorisce un **approccio integrato** alla gestione del rischio. I rischi non finanziari non sono più interpretati come ambiti separati, ma come **dimensioni tra loro interconnesse**.

Legal Risk

Rischi che comportano procedimenti legali, inclusi mancato rispetto (o elusione) di obblighi normativi, contrattuali ed etici, nonché eventi di misconduct.

Misconduct
Condotte improrie/ fraudolente nei cofronti di clienti e mercato

Non Misconduct
Altri rischi legali (es: mancato rispetto di obblighi contrattuali)

ICT Risk

Rischi connessi all'uso di sistemi e tecnologie informatiche che possono compromettere la sicurezza, l'operatività o la continuità dei servizi.

Cyber
Rischi riconducibili ad attacchi informatici

Non Cyber
Altri rischi ICT (es: guasti HW, errori SW, obsolescenza)

ESG & Greenwashing

Rischi di impatti finanziari negativi, attuali o prospettici, derivanti dall'influenza dei fattori ambientali, sociali e di governance.

ESG
Fattori esterni climatici, sociali e di governance

Greenwashing
Comunicazioni/azioni sulla sostenibilità non accurate o fuorvianti rispetto al reale profilo ESG

Business Continuity

Rischi derivanti dall'incapacità di garantire e mantenere adeguati framework di business continuity.

Resilience Failure
Inefficacia dei piani di risposta e ripristino o incapacità di mantenere l'erogazione dei servizi a seguito di un evento disruptive

Fraud Risk

Rischio di subire perdite economiche o reputazionali a seguito di comportamenti fraudolenti interni o esterni.

Identy Management

Access
Gestione inadeguata delle credenziali e dei privilegi di accesso (es. eccessivi o non aggiornati), con aumento del rischio di accessi non autorizzati.

Third-Party Risk

Rischi derivanti dall'utilizzo di servizi forniti da terze parti o dai loro subfornitori, inclusi i casi di outsourcing.

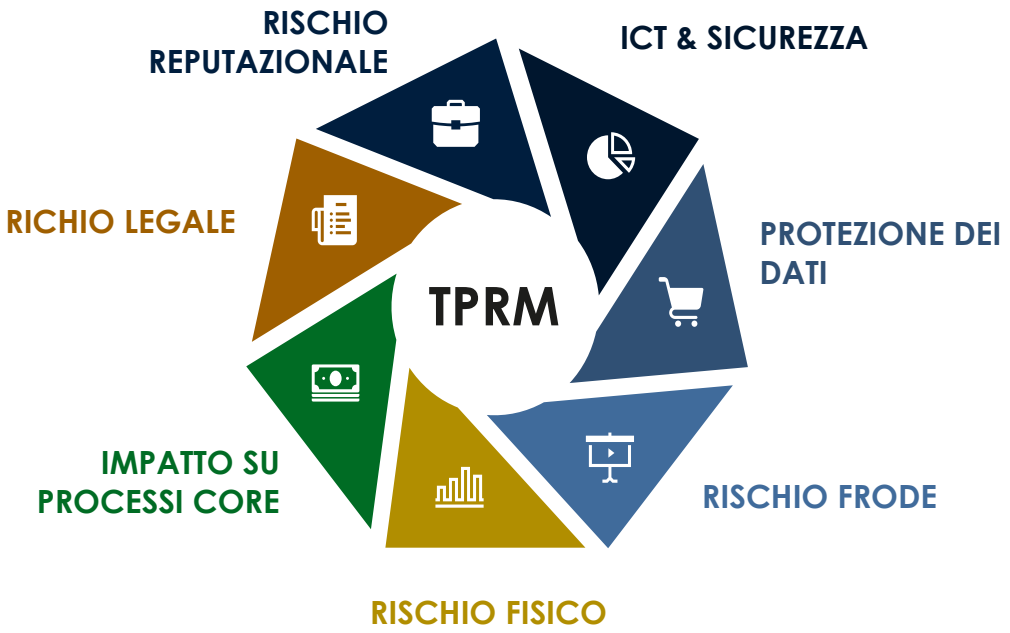
Supply Chain &Vendors
Carenze nella gestione della relazione con il fornitore e inadeguata gestione dei rischi connessi alla terza parte (selezione e due diligence, contratti e SLA, monitoraggio).

- I rischi non finanziari sono trasversali e interconnessi
- Nei rapporti con terze parti, tali rischi convergono
- L'esposizione della banca si concentra lungo la supply chain

Il **TPRM richiede** una **lettura e** una **gestione integrata** dei rischi non finanziari

Il Framework TPRM: una leva trasversale di integrazione

Le terze parti rappresentano un efficace **punto di convergenza dei rischi non finanziari**; il Framework **TPRM** consente di gestirli in modo **integrato** lungo l'intero ciclo di vita dei rapporti con il fornitore.



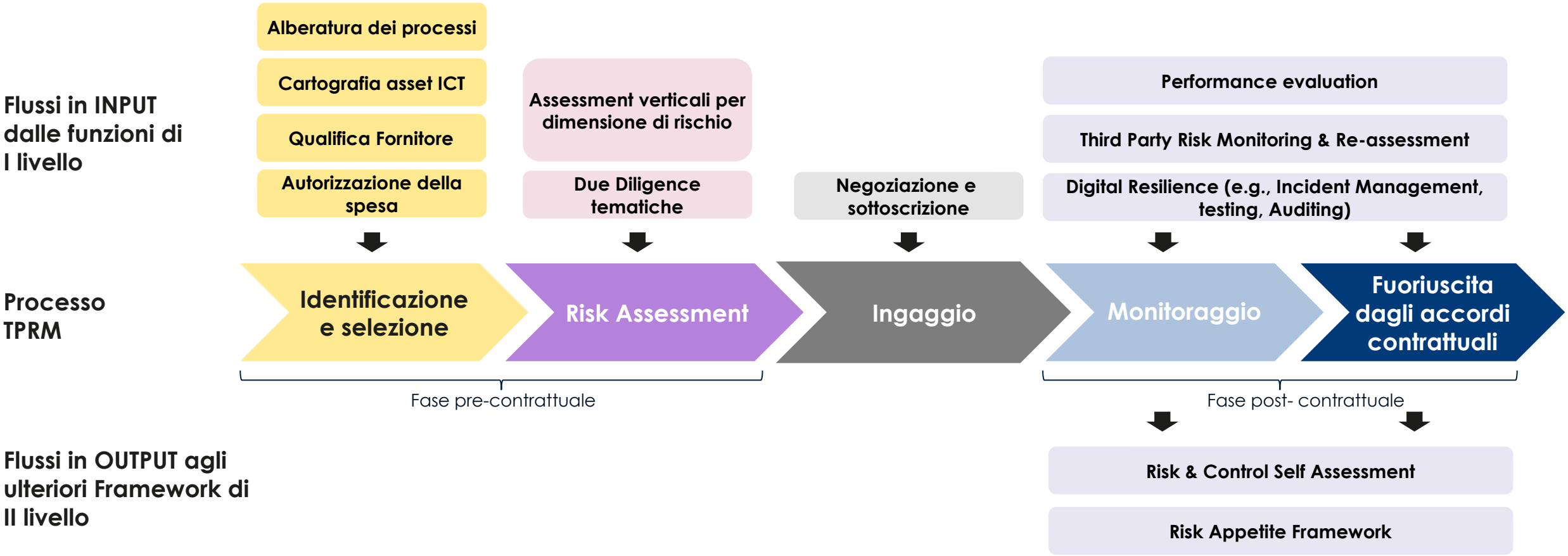
Il Framework TPRM abilita:

- **Identificazione dei rischi** connessi agli ambiti (processi, funzioni) nelle quali sono impiegate Terze Parti;
- **Valutazione dei rischi specifici connessi alle Terze Parti** (solidità finanziaria, reputazionale, profilo cyber, etc.)
- **Valutazione verticale delle singole dimensioni di rischio,** in funzione della crescente rilevanza dei servizi erogati da provider specializzati;
- **Integrazione** delle diverse dimensioni di rischio in una **valutazione complessiva**, cogliendo le **interconnessioni tra i singoli fattori;**
- **Monitoraggio e rivalutazione nel continuo dei rischi**, con un focus sull'impatto complessivo sulla **resilienza della Banca**.

Il **TPRM** rappresenta il **layer di aggregazione** dei rischi non finanziari lungo **il ciclo di vita delle relazioni con terze parti.**

Dall'integrazione metodologica alla governance di processo

Il framework TPRM, caratterizzato **dall'analisi di molteplici dimensioni di rischio**, si fonda su un **processo interconnesso** che favorisce la circolazione e la **condivisione dei flussi informativi da e verso altri processi/framework di valutazione e gestione del rischio.**



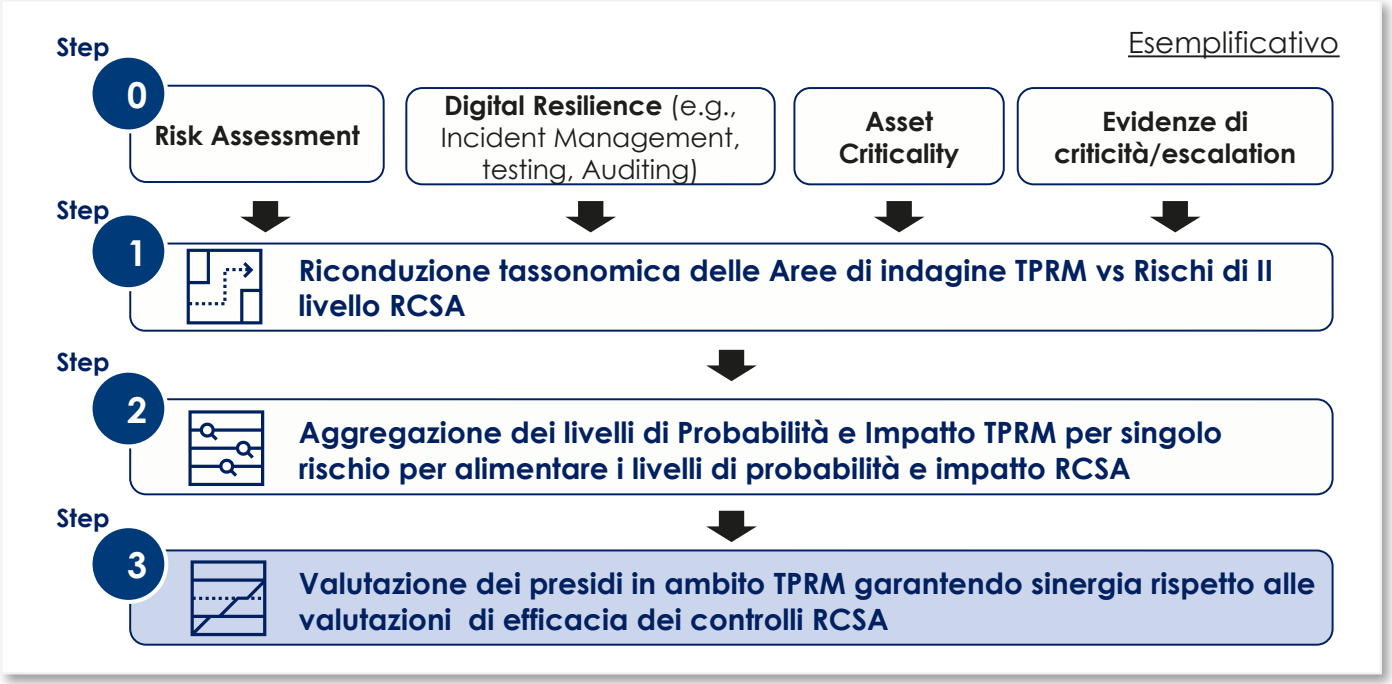
Il TPRM si integra nei processi di gestione del rischio

La valutazione dei rischi e dei controlli della Banca si basa su una tassonomia condivisa. In tale ambito, il **TPRM recepisce gli elementi di criticità e rischio** propri del **contesto operativo** in cui la terza parte opera (processi, asset, persone e strutture) e li analizza in funzione della capacità del fornitore di mitigare tali rischi. Sono inoltre considerati **specifici fattori di rischio** legati alla terza parte, quali **lock-in**, esigenze di **step-in**, **concentrazione** e dipendenze da **subfornitori**.

Ne consegue che le **valutazioni di rischio e di efficacia dei controlli condotte nell'ambito del TPRM costituiscono input rilevanti per gli altri processi di gestione del rischio**, tra cui, in primis, il Framework di RCSA della Banca.

Intesa Sanpaolo ha pertanto definito:

- un approccio volto alla **riconduzione** delle **valutazioni di rischio ed efficacia dei controlli** effettuate nel contesto del Framework TPRM (contract-based)
- **assicurando che tali valutazioni confluiscano** all'interno in un più ampio framework di valutazione e gestione dei rischi non finanziari, garantendo le opportune sinergie.



Il contributo TPRM al Framework di reporting Integrato

L'integrazione dei rischi non finanziari si realizza anche attraverso un **framework di reporting condiviso e metodologicamente allineato**. In questo ambito, il **TPRM** rappresenta una **fonte strutturata di dati e misure di rischio**, pienamente **integrabili** nei flussi di reporting e riutilizzabili nei processi di risk management, inclusi quelli di RCSA.

Viste «contract –based»

Metriche accordo contrattuale

- ***Rischio inerente del servizio*** *- Il contratto ha ad oggetto un servizio con un livello rischio inerente valutato come «materiale» (e.g., pari o superiore a «Medio Alto»)*
- ***Servizio a supporto/non a supporto di FEI -*** *L'accordo contrattuale ha ad oggetto un servizio a supporto di Funzioni Essenziali o Importanti*
- ***Rilevanza del servizio per area di rischio -*** *Il contratto ha ad oggetto un servizio rilevante per una determinata area di rischio (e.g., Sicurezza Informatica.)…*

Accordi contrattuali – viste di sintesi

Livello di rischio per singolo accordo

Metriche su Terza Parti Single Name

- ***Rischi prevalenti del fornitore*** *- Il contratto prevede l'esternalizzazione/ fornitura di un servizio ad un provider avente una valutazione di Due Diligence negativa*
- ***Rischio Paese -*** *Il provider ha sede in un paese classificato come ad alto rischio*

Due Diligence per fornitore e distribuzione aggregata

Viste «portfolio–based»

Metriche portafoglio accordi

- ***% di rischio inerente di portafoglio -*** *Quota di servizi in portafoglio aventi un rischio inerente «materiale»*
- ***% di servizi a supporto di FEI*** *- Quota di accordi contrattuali in portafoglio aventi ad oggetto servizi a supporto di FEI*
- ***% di accordi di esternalizzazione/ fornitura*** *in portafoglio*
- ***Processi di eccezione -*** *Processi di escalation attivi alla data di riferimento*
- ***Piani di rimedio -*** *Ratio 'piani di rimedio conclusi/ piani di rimedio definiti'*
- …

Portafoglio contratti – distribuzione per rischio

Efficacia dei presidi del fornitore

Metriche Portafoglio Terze Parti

- ***Rischio di concentrazione*** *- Livello di rischio di concentrazione del portafoglio di Terze Parti del Gruppo*
- ***Rischio di aggregazione*** *- Livello di rischio di aggregazione (e.g., % di servizi della stessa tipologia/ ramo di business) del portafoglio di Terze Parti del Gruppo*
- ***Rischio ESG*** *- % di provider del Gruppo aventi uno score ESG valutato come «negativo»*

Viste regolamentari e focus su fornitori critici

La gestione integrata del rischio è supportata da soluzioni tecnologiche

L'evoluzione verso un modello integrato di gestione dei rischi non finanziari richiede **l'adozione di soluzioni tecnologiche** in grado di abilitare l'automatizzazione e la **scalabilità dei processi TPRM.**

In tale contesto, la **digitalizzazione dei flussi e la strutturazione delle basi dati** costituiscono **elementi chiave** per migliorare l'efficienza operativa e garantire la sostenibilità nel continuo del modello.

- **Automazione delle attività core -** Standardizzazione delle logiche di valutazione e riduzione degli interventi manuali lungo il ciclo di vita TPRM
- **Riutilizzo e valorizzazione del dato -** Sfruttamento sistematico delle informazioni pregresse e centralizzazione delle evidenze di rischio per abilitare la valutazione dei rischi nel continuo (continuous improvement)
- **Integrazione dei flussi informativi -** Allineamento tra processi TPRM e framework di risk management (es. RCSA) attraverso basi dati e metriche condivise
- **Supporto al reporting evoluto -** Disponibilità di insight tempestivi, coerenti e aggregabili, a supporto di una rappresentazione integrata del rischio
- **Efficienza e sostenibilità del modello operativo -** Riduzione dei tempi di processo, maggiore scalabilità e contenimento degli effort operativi

L'adozione di soluzioni basate su **Artificial Intelligence** consente di **accelerare e industrializzare** il processo di Risk Assessment, sfruttando le informazioni disponibili in modo destrutturato e **riducendo in modo significativo tempi ed effort operativi.**

Principali implicazioni

- **Dai verticali di rischio al framework integrato di Non-Financial Risk**: l'evoluzione regolamentare e la crescente complessità del contesto esterno (e.g., rischio geopolitico) richiedono una gestione olistica, in grado di coglierne interrelazioni e dinamiche evolutive, considerando anche nuovi fattori di rischio legati all'utilizzo di tecnologie avanzate (e.g., digital asset, artificial intelligence).

- **Il ruolo centrale dei dati nella gestione dei rischi TPRM:** le valutazioni di rischio in ambito Terze Parti non possono prescindere da una solida base dati che fattorizzi informazioni rivenienti dai processi di I livello di gestione del rischio (e.g., incident management, data governance, privacy, sicurezza fisica e informatica, evidenze circa ispezioni condotte sul fornitore); il riutilizzo di tali informazioni è altrettanto centrale nella valutazione del rischio TPRM in quanto abilita il monitoraggio continuo dei rischi (continuous improvement) e una gestione proattiva degli accordi contrattuali, intercettando tempestivamente potenziali criticità e scalando, ove opportuno, le situazioni di rischio più rilevanti.

- **Reporting integrato come leva di governo:** affiancare viste verticali sul singolo rischio e trasversali per una lettura integrata. In ambito TPRM, una combinazione di viste «contract-based» e «portfolio-based» supportano la realizzazione dell'Integrated Reporting.

- **Raccordo TPRM ↔ RCSA per abilitare le sinergie:** necessaria una riconduzione tassonomica e regole di aggregazione per portare le evidenze TPRM all'interno dei più ampi framework di gestione del rischio (e.g., RCSA).

- **Leva tecnologica per efficienza e sostenibilità:** standardizzazione delle logiche di valutazione, valorizzazione del patrimonio informativo storico e automatizzazione delle attività ricorrenti, con l'obiettivo di rendere il modello operativo più efficiente, scalabile e sostenibile nel tempo.

- **AI come acceleratore del framework TPRM:** modelli esperti e logiche di automazione abilitano un processo scalabile e data-driven, mantenendo il presidio umano come elemento chiave di governo e accountability.


INTESA
SANPAOLO