



**INTESA**  **SANPAOLO**

# La Governance dei Rischi Non Finanziari in Intesa Sanpaolo

**Domenico Fileppo**  
Executive Director  
Operational, IT & Cyber Risk Management

Supervision Risks & Profitability 2024  
Sessione Parallela 2.3  
La buona governance di fronte ai rischi emergenti  
Milano, 12 Giugno 2024

# Agenda



**Non-Financial Risk in Intesa Sanpaolo**



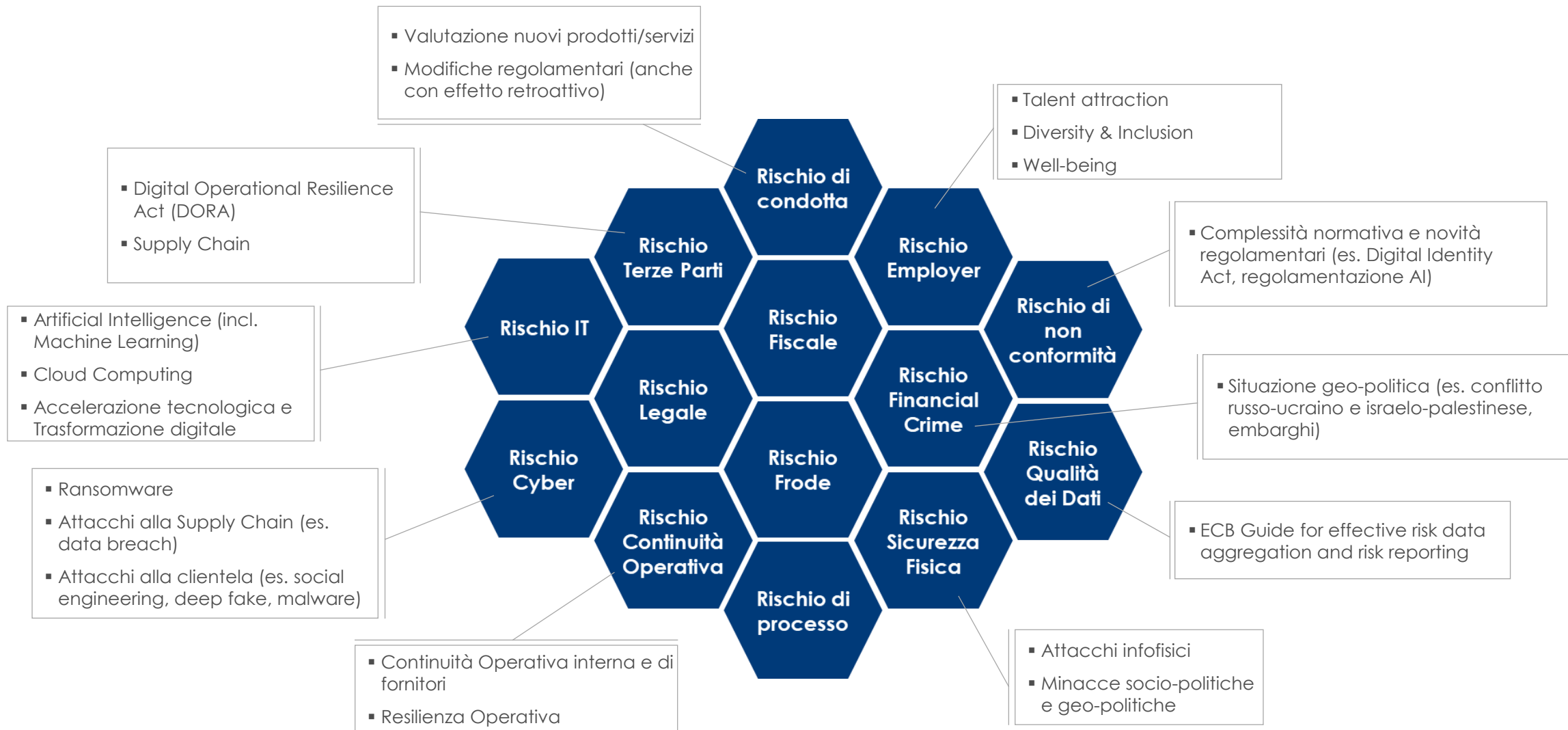
**Operational, ICT and Security Risk Framework**



**Lessons learnt**



# Molti dei rischi inclusi tra i rischi non finanziari<sup>1</sup> sono in rapida evoluzione e, di conseguenza, deve essere valutato con attenzione il relativo profilo di rischio



1. I rischi non finanziari si inseriscono nella complessiva Group Risk Inventory di Gruppo e non includono i rischi strategici e reputazionali e ESG

# Tra i rischi non finanziari più rilevanti, analisi interne ed esterne collocano i rischi ICT, di Sicurezza e delle terze parti nelle prime posizioni



## Valutazione esterna

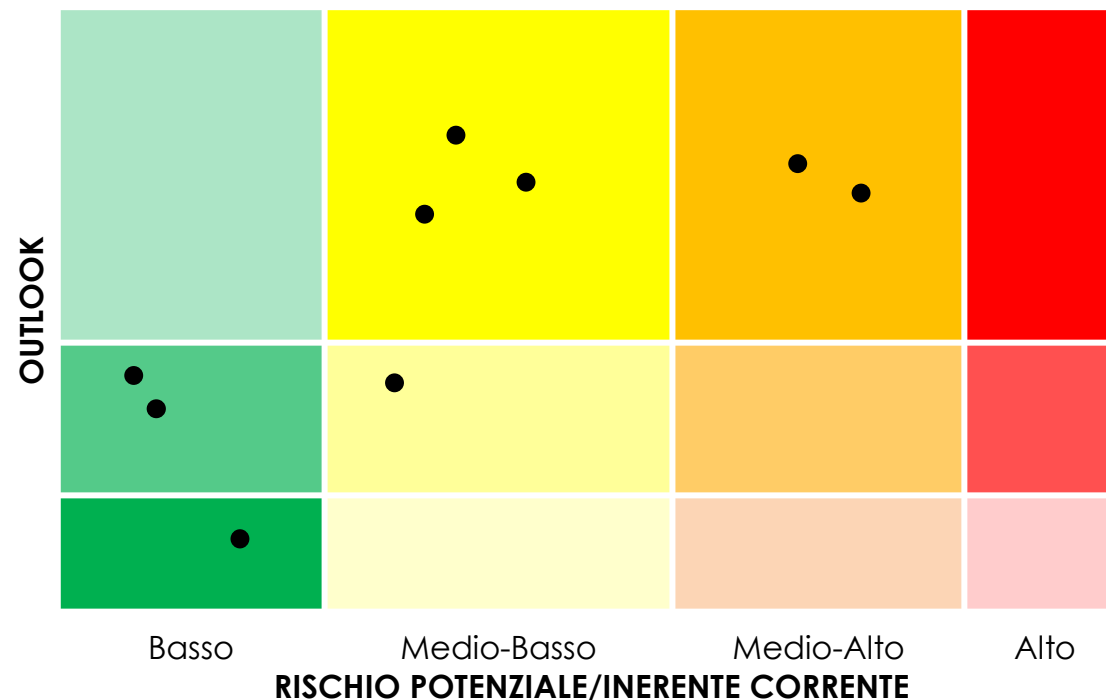
- 2023-25 ECB Banking Supervision priorities** suggerisce l'indirizzo delle lacune individuate:
  - nelle **strategie** di **trasformazione digitale**
  - sull'**operational resilience** (es. cyber risks, outsourcing)
  - nella capacità del **management** di effettuare **steering**
- La **survey 2024** dell'**associazione ORX<sup>1</sup>** sulla **valutazione** dei **rischi emergenti** e più **significativi** che attualmente impattano i settore finanziario ha confermato il rischi **ICT, di sicurezza** e delle **terze parti** nelle prime posizioni

ORX – Rischi emergenti e materiali per il settore finanziario (2024)	
1°	Information Security (incl. cyber)
2°	Technology
3°	Business Continuity (incl. 3 <sup>rd</sup> Party)
4°	Compliance regolamentare
5°	Data Management
6°	Climate
7°	Third Party
8°	People
9°	Frodi (interne ed esterne)
10°	Condotta

## Valutazione interna

Il Gruppo Intesa Sanpaolo effettua internamente una valutazione corrente e prospettica (**Strategic Risk Assessment**) dei rischi inclusi nella Group Risk Inventory e la aggiorna **con cadenza annuale**

L'ultimo aggiornamento ha evidenziato una percezione sostanzialmente in linea con quella consortile

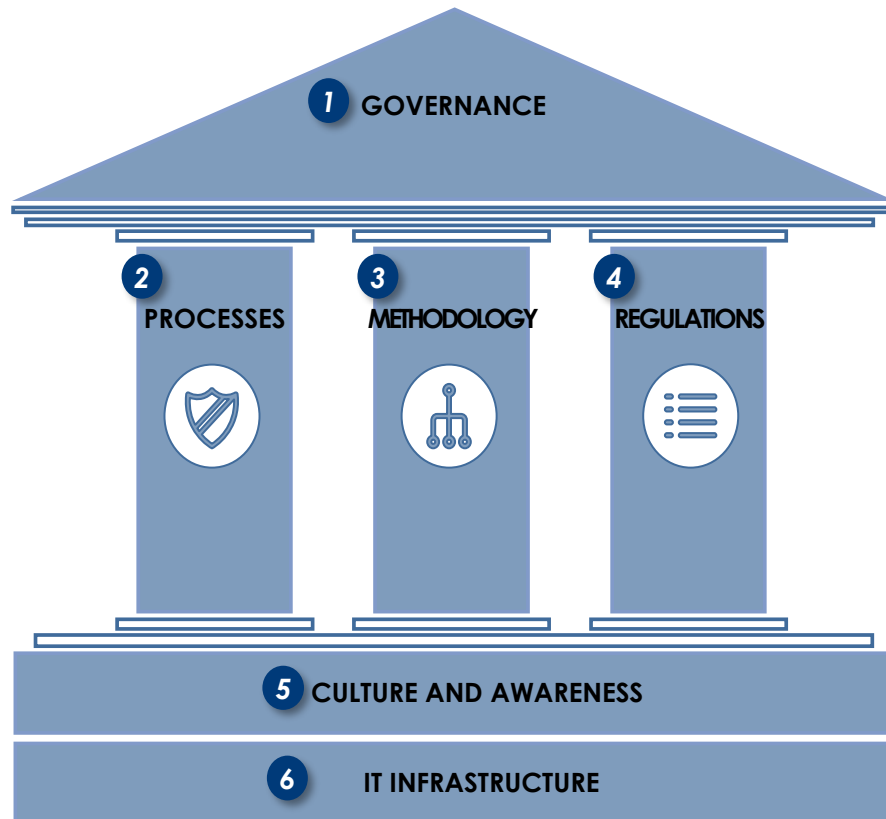


1. O.R.X. ("Operational Riskdata eXchange Association - ORX è la più grande associazione di operational risk management association nel settore dei servizi finanziari dal 2002")

# Il framework per la gestione dei rischi Operativi, ICT e di Sicurezza è organizzato in sei pillar principali



4



- 1 Insieme di **obiettivi** e **strategie** (es. RAF) di gestione dei rischi Operativi, ICT e di Sicurezza, di **ruoli** e **responsabilità** delle funzioni coinvolte e delle loro interazioni
- 2 Insieme di **processi** a supporto della gestione dei rischi Operativi, ICT e di Sicurezza (incluse **soluzioni e strumenti** organizzativi/tecnologici)
- 3 Insieme di **metodologie** per la valutazione dell'esposizione ai rischi Operativi, ICT e di Sicurezza
- 4 Insieme di documenti (**regole, manuali e linee guida**) che regolano la gestione dei rischi Operativi, ICT e di Sicurezza, definiti a livello di Gruppo e adattati alle esigenze locali, ove necessario
- 5 Insieme di iniziative volte a diffondere la **cultura** dei rischi Operativi, ICT e di Sicurezza in tutto il Gruppo e ad aumentare il livello di **consapevolezza** circa la loro rilevanza
- 6 **Infrastruttura IT, estesa a tutto il Gruppo** (incluso il perimetro assicurativo), a supporto dei processi chiave



# Nel corso degli ultimi anni la tassonomia dei rischi che rientrano nel più ampio perimetro dei rischi non finanziari si è molto arricchita, sia a seguito delle evoluzioni regolamentari che per esigenze gestionali

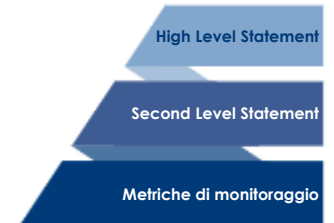
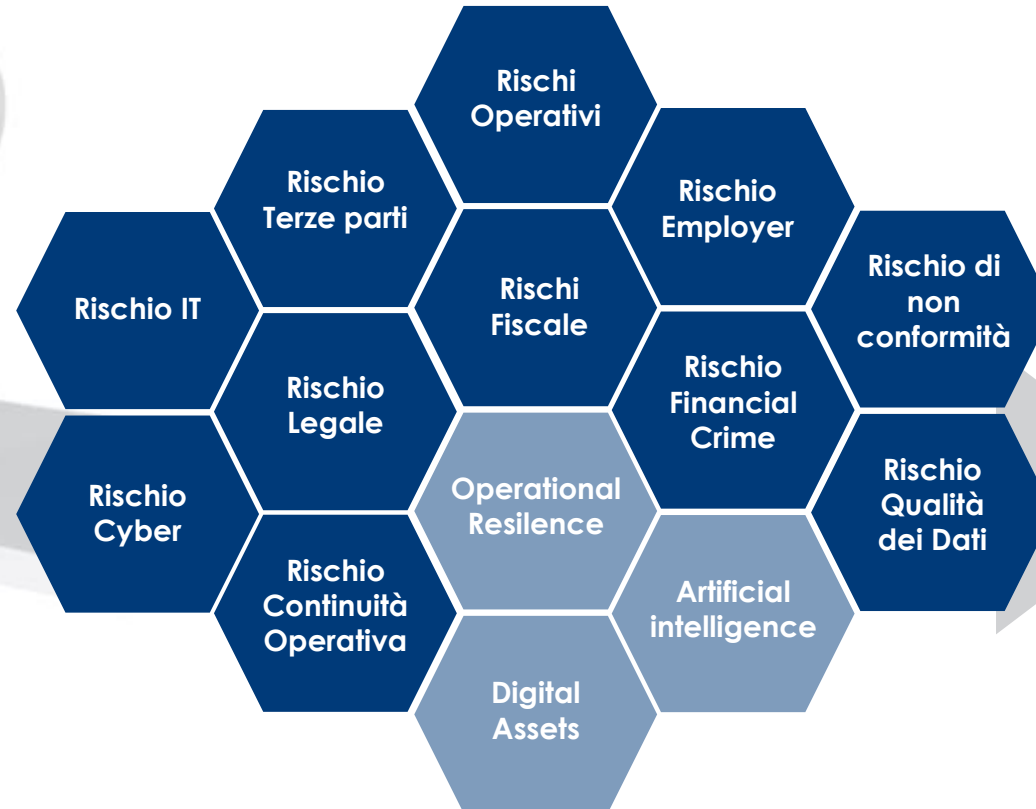


**2015**



**2024**

*Il Risk Appetite Framework per i rischi non finanziari ad oggi è articolato in 11 sezioni riferibili a specifici rischi + 3 sezioni dedicate a fenomeni emergenti*



- **32 Metriche con limiti** (Early Warning, Soft Limit, Hard Limit)
- **34 indicatori**

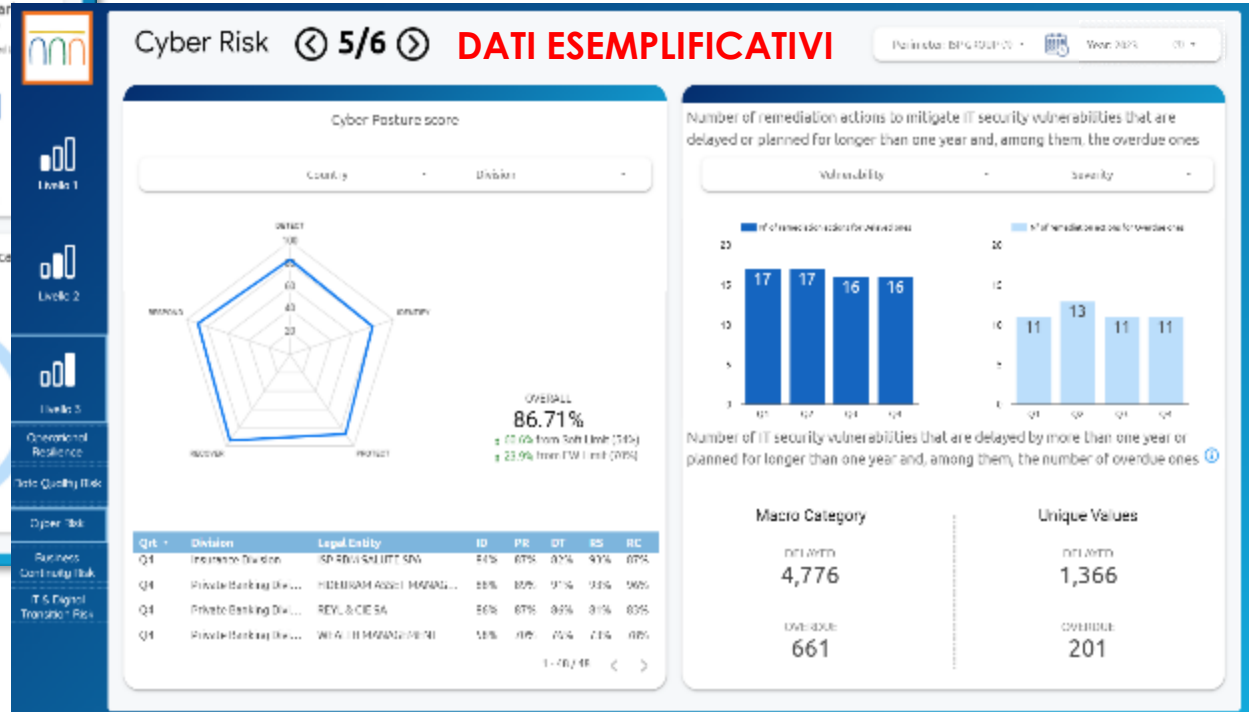
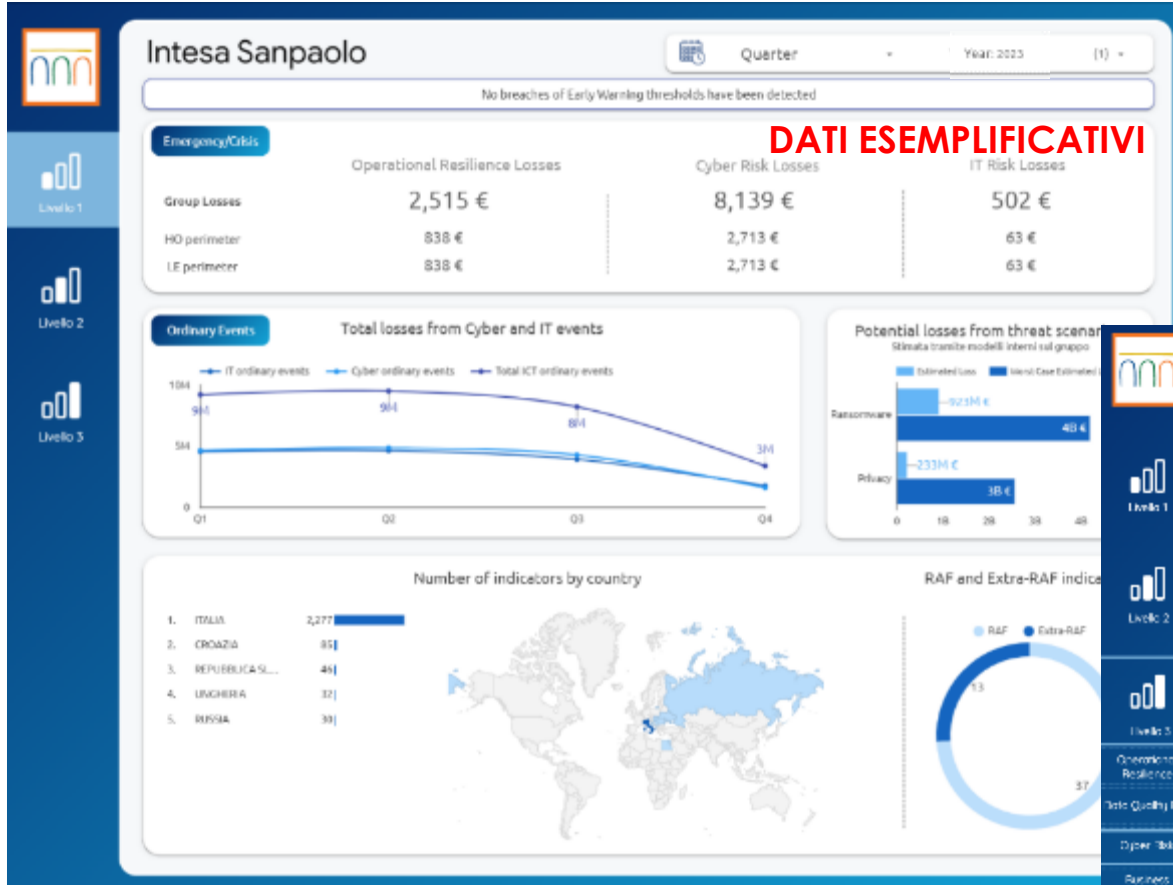
*Molte delle metriche sono oggetto di cascading su diversi perimetri del Gruppo*



# Per rafforzare il presidio della governance dei rischi non finanziari sono state introdotte delle dashboard di monitoraggio di metriche ed indicatori



GOVERNANCE

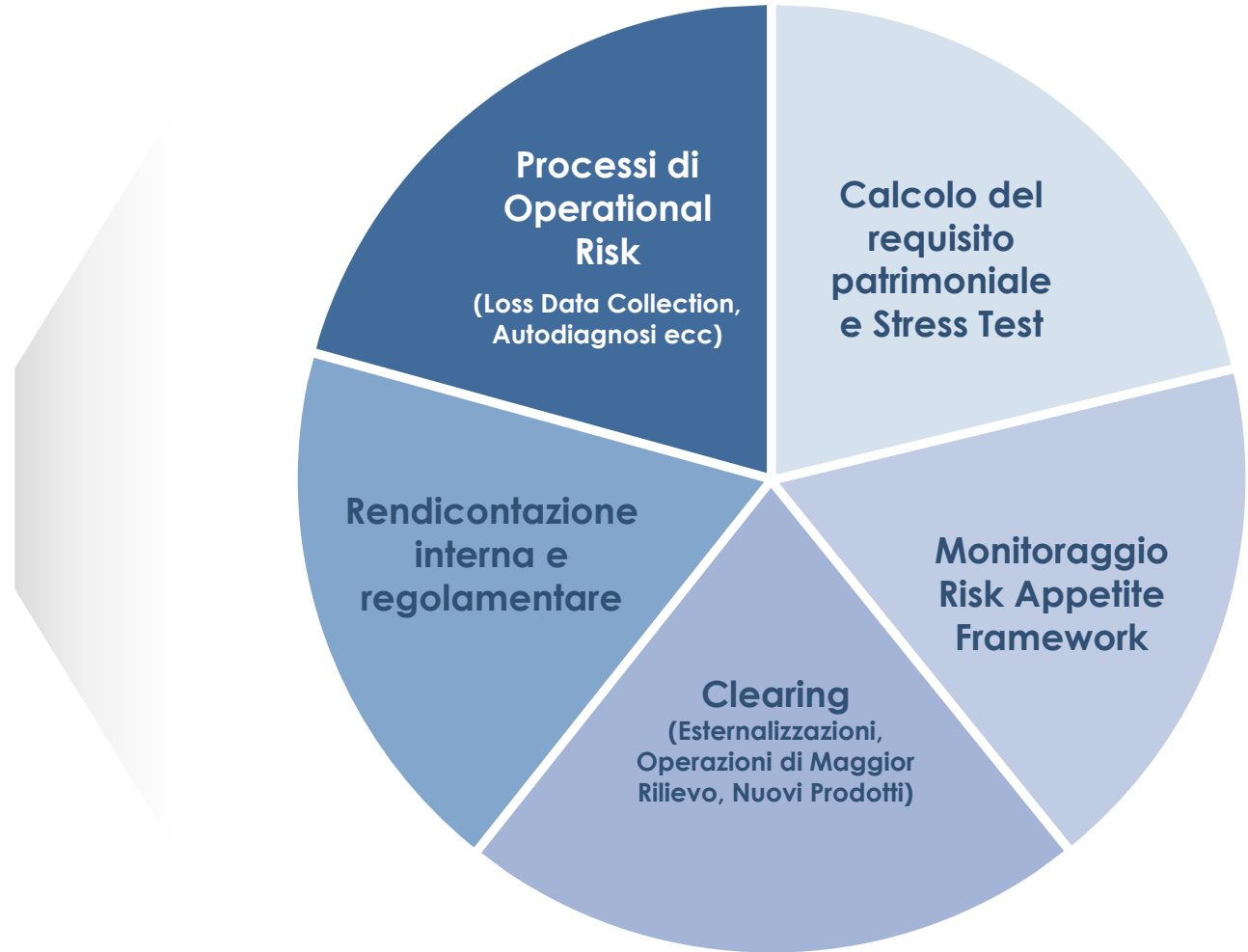
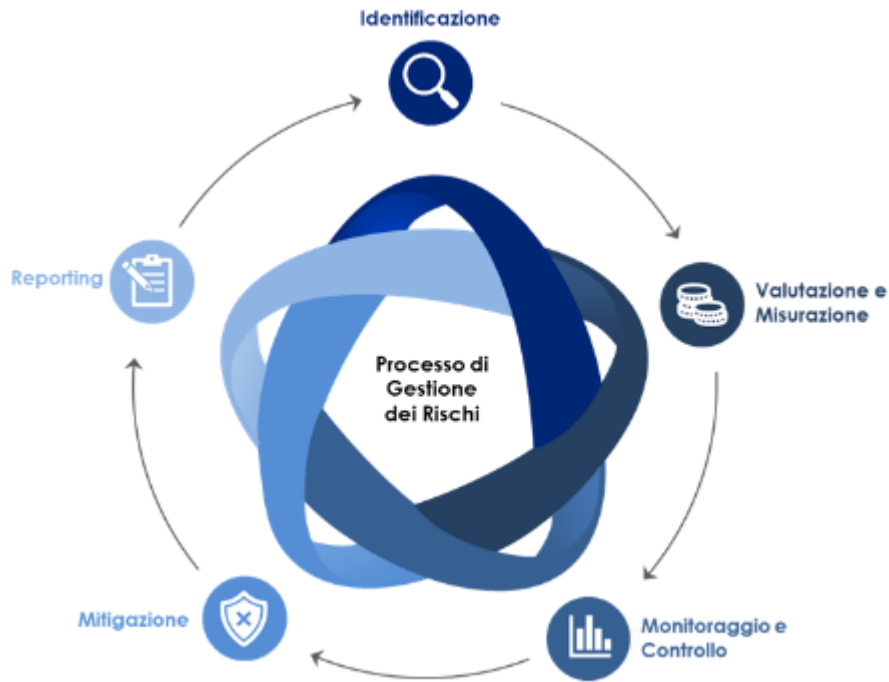




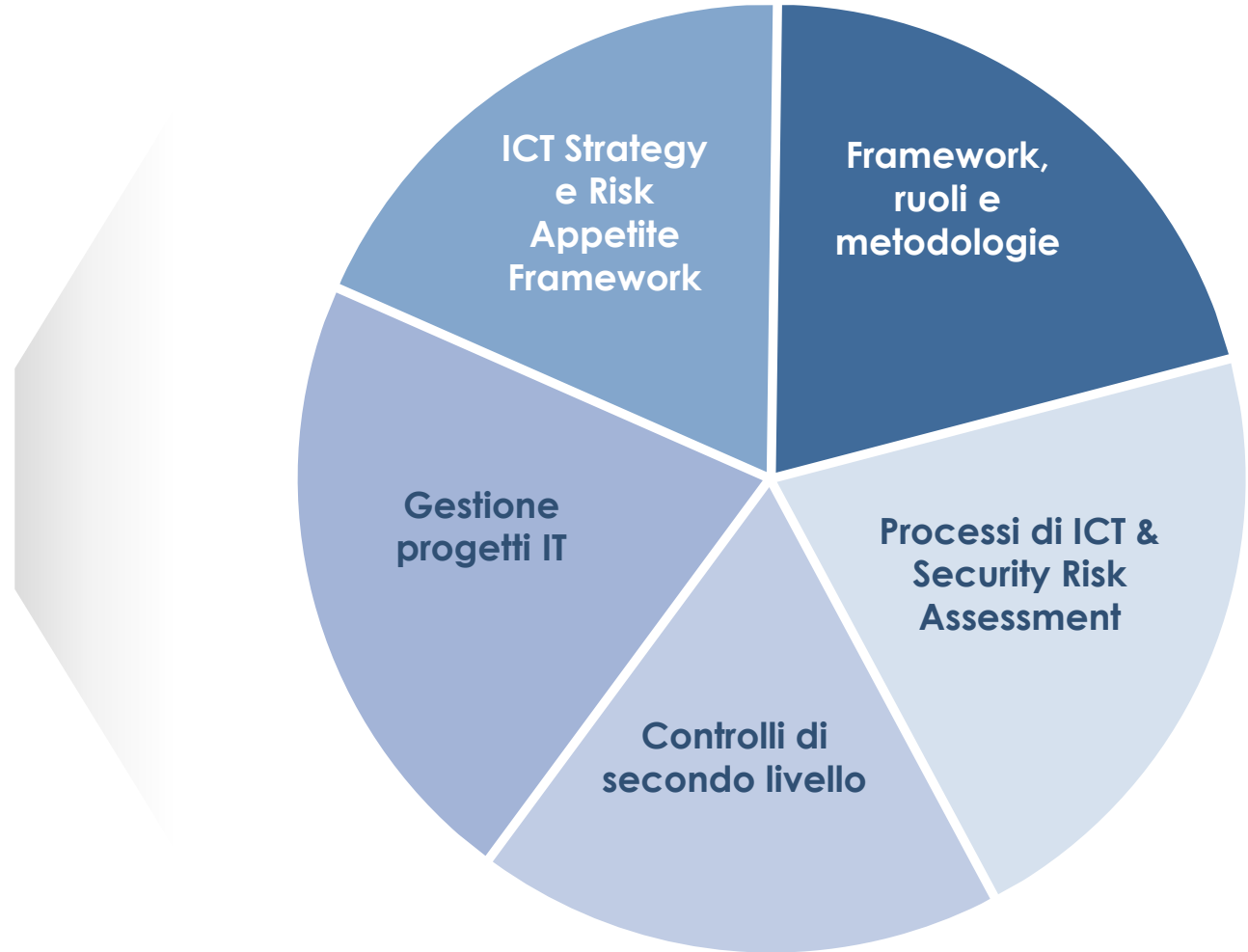
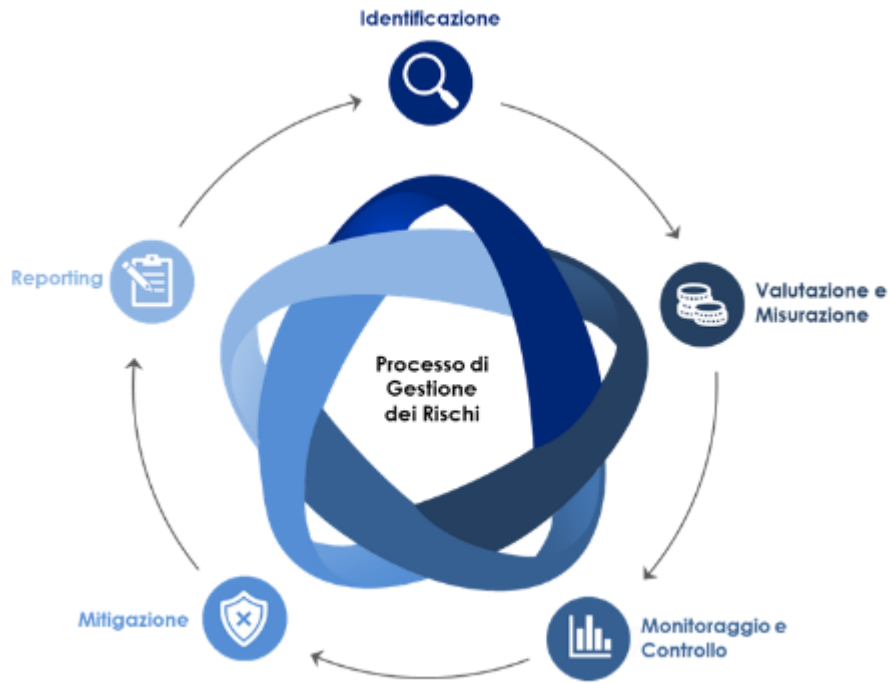
# Il processo di gestione dei rischi è organizzato in fasi cui si possono ricondurre le attività previste dal framework di governo dei rischi operativi...



PROCESSES








# Il contesto dei rischi non finanziari dovrà essere sempre più supportato da modelli volti a prevedere eventi avversi (ad es. a bassa frequenza e alto impatto) e metodologie e framework che consentano di reagire a eventi ignoti e nuovi rischi

- I **modelli a supporto della valutazione e gestione dei rischi non finanziari stanno progressivamente evolvendo**, per diventare **strumenti a supporto dell'identificazione di fenomeni e trend emergenti e quindi identificazione di rischi emergenti**. In altri termini, l'obiettivo è sfruttare algoritmi e tecniche avanzate per **anticipare elementi non noti** e trend futuri.
- Questo **cambio di paradigma** è guidato in Intesa Sanpaolo da un **approccio data driven** dall'utilizzo di **strumenti analitici** di frontiera

<p><b>Unknown-Knowns</b> (fatti nascosti)</p> <ul style="list-style-type: none"> <li>▪ Elementi non ancora noti</li> <li>▪ Sconosciuti a noi, ma conosciuti ad altri</li> </ul>	<p><b>Unknown-Unknowns</b> (rischi sconosciuti)</p> <ul style="list-style-type: none"> <li>▪ Elementi non ancora noti</li> <li>▪ Sconosciuti a noi e ad altri</li> </ul>
<p><b>Known-Knowns</b> (fatti e requisiti)</p> <ul style="list-style-type: none"> <li>▪ Non sono rischi</li> <li>▪ Elementi gestiti come parte del perimetro di progetto</li> </ul>	<p><b>Known-Unknowns</b> (rischi conosciuti)</p> <ul style="list-style-type: none"> <li>▪ Rischi classicamente intesi</li> <li>▪ Sono noti probabilità e impatto dei rischi</li> </ul>

**Qualche esempio...**

- **Metodologie relative a processi di gestione dei rischi operativi, ICT e di Sicurezza**  
*Analisi di Scenario, RCSA*
- **Altre metodologie correlate ai rischi non finanziari**  
*Scoring Terze Parti, Cyber Risk, ICT, Business Resilience, Conformità....*





CULTURE



# La spinta trasformativa e i continui cambiamenti del panorama ICT e di Sicurezza richiedono un'attenzione particolare all'aggiornamento della normativa interna e all'attuazione di iniziative di formazione e risk awareness

## Normativa

### Highlights



**15+**  
linee guida

**40+**  
regole

## Cultura

### Highlights



**5+**  
Moduli di training dedicati alla diffusione della cultura sui rischi

**5+**  
Webinar organizzati nell'ultimo anno su Risk Culture e Awareness

## Formazione

### Highlights



**250+**  
Ore di formazione specifica su tematiche relative a rischi Operativi, ICT e di Sicurezza

## People



*Preparazione e Resilienza sono gli elementi essenziali della capacità di una banca di affrontare in maniera efficace una crisi*

# Anche i processi di gestione del rischio devono essere rivisti in un'ottica di maggiore digitalizzazione e applicazione di tecniche innovative

**PROCESS  
AUTOMATION**

**AI, ANALYTICS & DECISION  
AUTOMATION, GEN AI,  
DISRUPTIVE TECHNOLOGY**

**Operational, IT  
& Cyber Risk  
Management**

**SOUNDNESS  
ARCHITECTURE**

**DIGITAL CULTURE, SKILL &  
PROFESSIONS**

**ENHANCED DATA  
MANAGEMENT**

**Key words**

- ❖ Data driven
- ❖ Risk Digital Factory
- ❖ Regulatory sensing
- ❖ Supporto al Business
- ❖ Cloud
- ❖ Quantum
- ❖ Generative AI
- ❖ Low code
- ❖ Tribe, community

**BENEFICI**

**Inversione  
Piramide**



**Medio - Alto**

**Maggiore accuratezza  
modelli / controlli**



**Alto**

**Maggiore presidio  
dei rischi**



**Alto**

**Maggiore soddisfazione  
ed efficacia delle risorse**



**Medio - Alto**

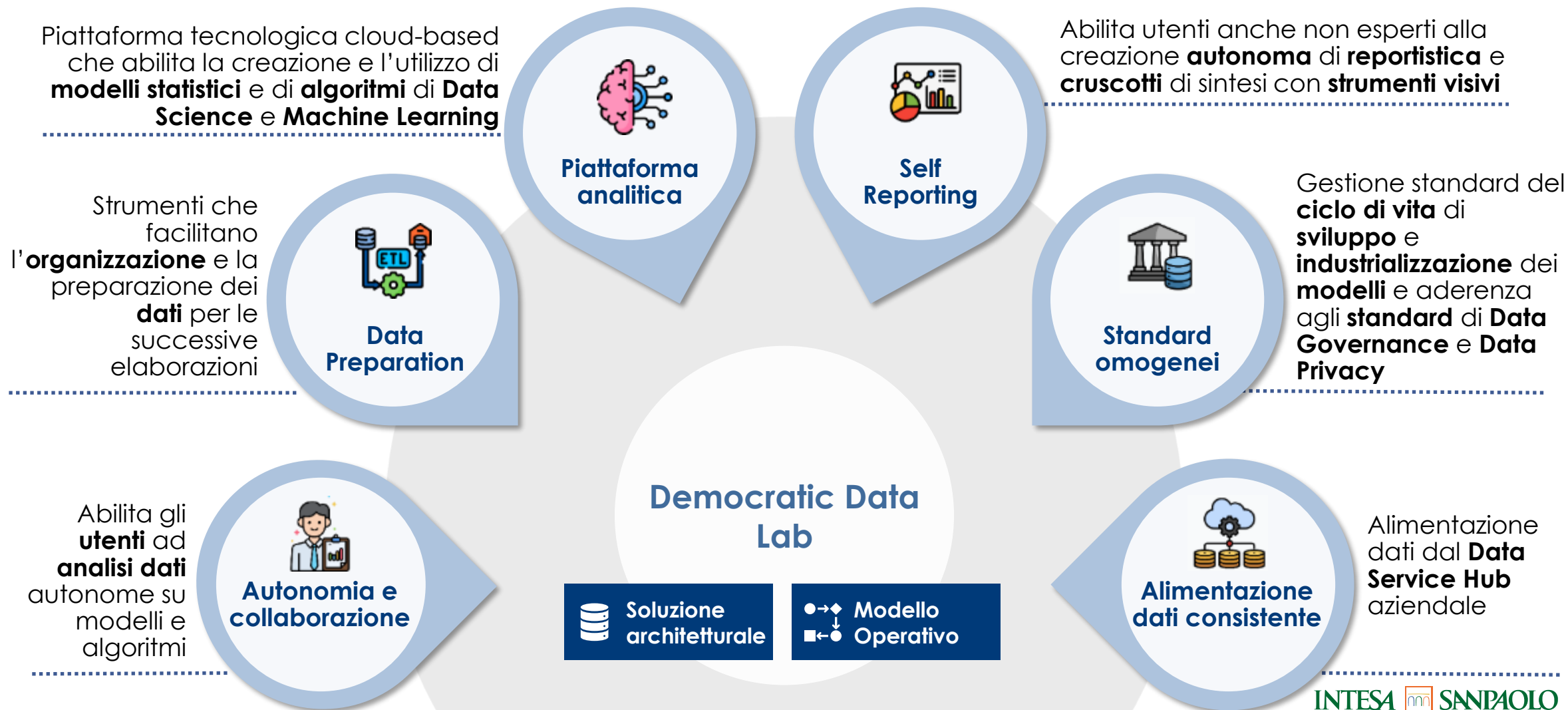
**RISCHIO A NON FARE INTERVENTO**

*La proliferazione di attività e della crescente mole di dati ad essa connessa richiederà un aumento di effort e costi. Basso efficientamento sull'ottimizzazione delle risorse e delle proprie competenze anche su attività a maggiore valore aggiunto*



**Medio - Alto**

# L'adozione di un nuovo strumento Cloud per democratizzare l'accesso a strumenti analitici evoluti si sta affiancando a quelli già utilizzati per iniziare a sviluppare modelli per la gestione dei rischi sconosciuti

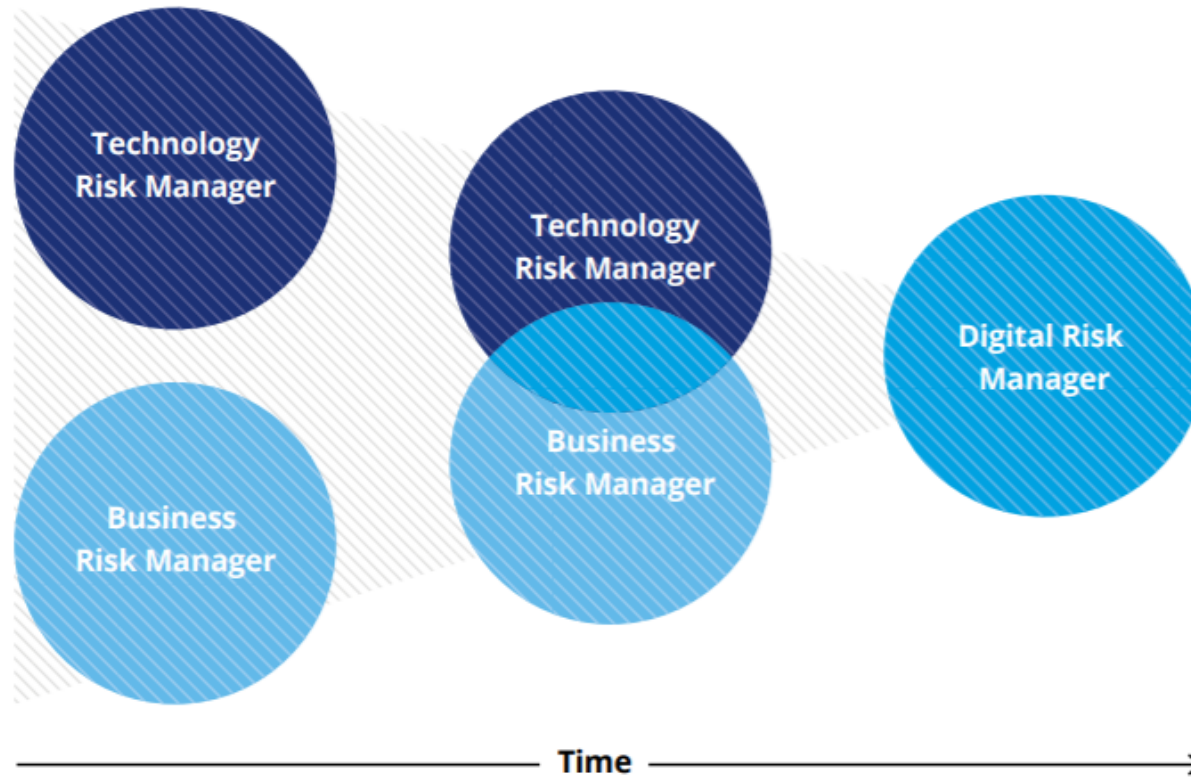


# Nel rafforzare la gestione dei rischi non finanziari, sono state identificate delle aree chiave (Governance, Digital & Data, Framework & Modelli e Persone) con alcune lesson learnt dirimenti...



Area	Elementi chiave
 Governance	<ul style="list-style-type: none"><li>▪ <b>Allineamento nel continuo</b> con <b>Board</b> per tutte le fasi del processo (dalle Strategie operative alla mitigazione delle issues ed al piano dei trattamenti)</li></ul>
 Digital & Data	<ul style="list-style-type: none"><li>▪ Definizione di una <b>strategia digitale complessiva</b> a livello di <b>Area CRO</b></li><li>▪ <b>Introduzione</b> di logiche <b>data-driven</b> nei <b>processi</b> attuali, volte ad oggettivare le valutazioni dei self-assessment e costituire una base su cui implementare controlli di secondo livello</li><li>▪ Adozione di <b>strumenti analitici evoluti</b> (es. Democratic DataLabs) e <b>strumenti</b> di <b>monitoraggio</b></li></ul>
 Framework & Modelli	<ul style="list-style-type: none"><li>▪ Adozione logiche «<b>by design</b>» anche su controlli di primo livello, sicurezza e resilienza operativa</li><li>▪ Setup di un <b>framework</b> di <b>controllo</b> di <b>secondo livello</b> e messa a terra delle attività operative di controllo</li><li>▪ Adozione del <b>Risk Control Self Assessment</b></li><li>▪ <b>Sviluppo</b> di <b>modelli</b> di <b>rischi non finanziari</b> forward-looking che puntano ad anticipare trend futuri e rischi emergenti (<i>unknown unknowns</i>)</li><li>▪ Evoluzione delle <b>metriche RAF</b> verso i <b>rischi emergenti</b> e più <b>rilevanti</b></li></ul>
 Persone	<ul style="list-style-type: none"><li>▪ Abilitare un <b>dialogo</b> «<i>streamless</i>» con le <b>funzioni tecniche</b> e <b>specialistiche</b> con «challenge» attivo</li><li>▪ Introduzione di nuove <b>figure professionali</b> ibride tra <b>Risk Manager</b> e <b>Technology Manager</b></li><li>▪ <b>Rafforzare</b> le iniziative di <b>education</b> sui <b>contenuti specialistici</b> di <b>maggior rilevanza</b> per i <b>rischi emergenti</b></li></ul>

... che affondano una comune radice sulla progressiva trasformazione culturale e di competenze verso la figura del Digital Risk Manager



Il **Digital Risk Manager** è la figura in grado di **comprendere** tutti gli aspetti del **ciclo di vita** dei **prodotti digitali** e che dispone di una **visione integrata** del **rischio** sia dal punto di vista di **business**, sia **tecnologico**