La Governance dei Rischi Non Finanziari in Intesa Sanpaolo

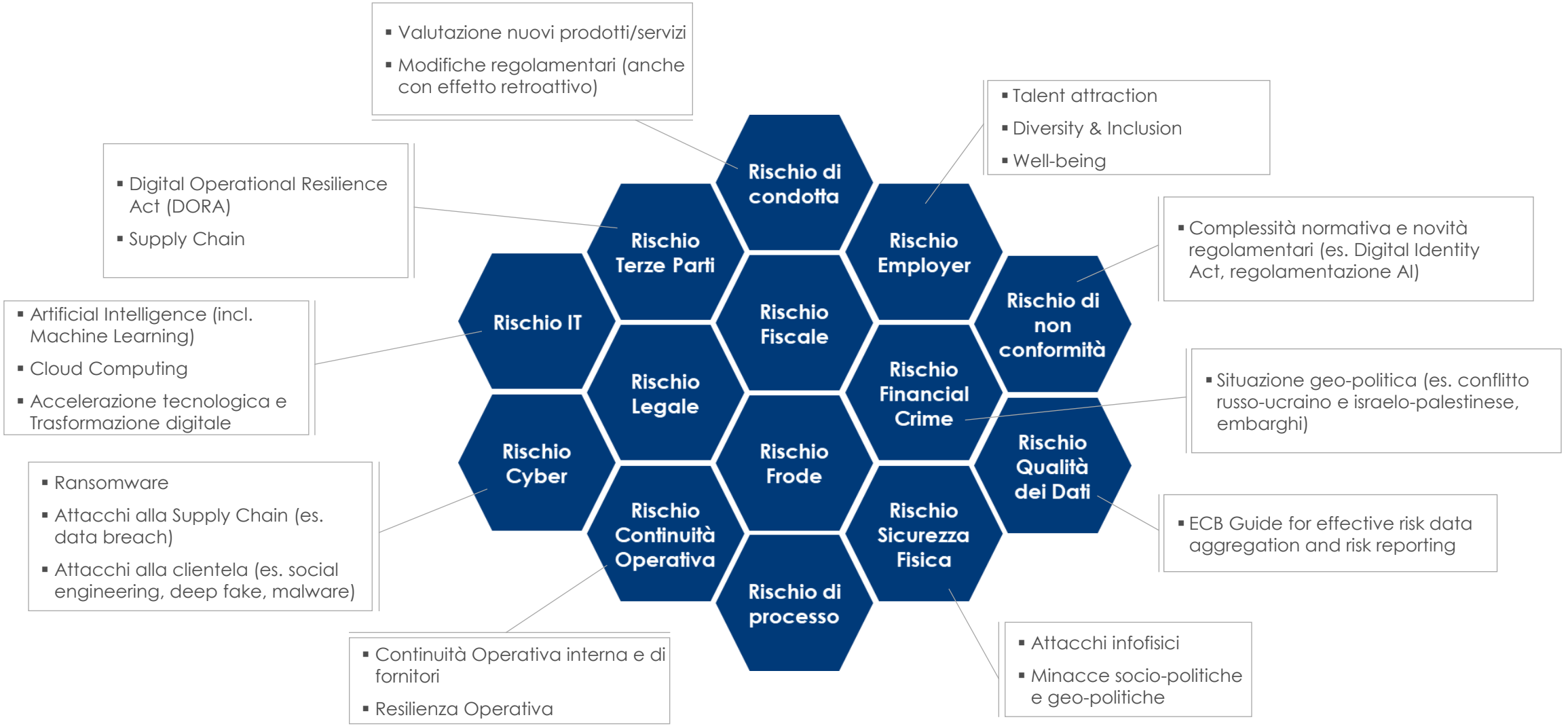
Domenico Fileppo
Executive Director
Operational, IT & Cyber Risk Management

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[1] 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**[1] 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

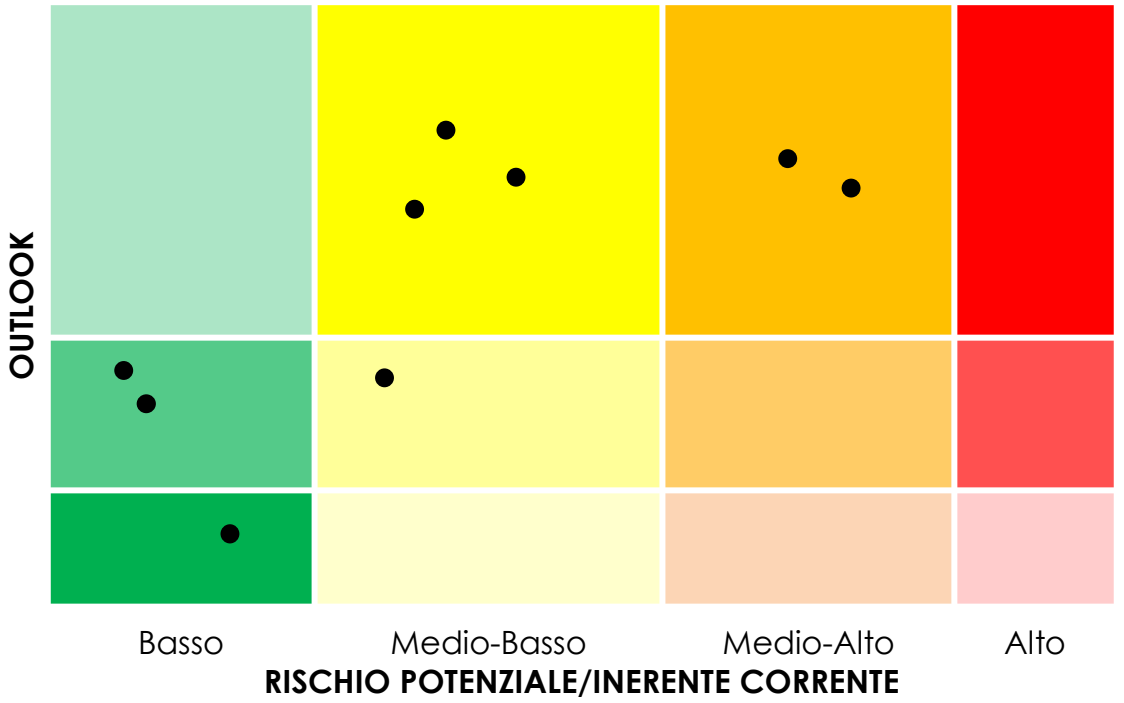
ORX – Rischi emergenti e materiali per il settore finanziario (2024)

1°	Information Security (incl. cyber)
2°	Technology
3°	Business Continuity (incl. 3rd Party)
4°	Compliance regolamentare
5°	Data Management
6°	Climate
7°	Third Party
8°	People
9°	Frodi (interne ed esterne)
10°	Condotta

Valutazione interna

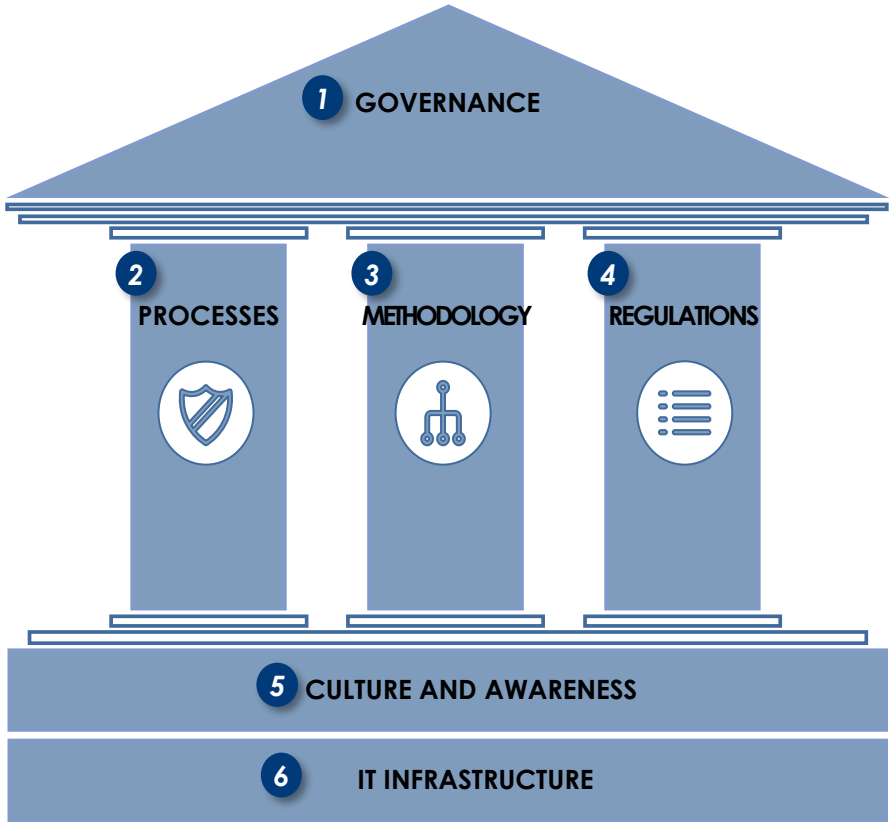
Il Gruppo Intesa Sanpaolo effettua internamente una valutazione corrente e prospettica (**Strategic Risk Assessment)** dei rischi inclusi nella Group Risk Inventory e la aggiorna **con cadenza annuale**

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")

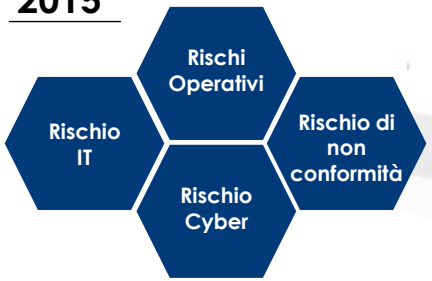
Il framework per la gestione dei rischi Operativi, ICT e di Sicurezza è organizzato in sei pillar principali



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

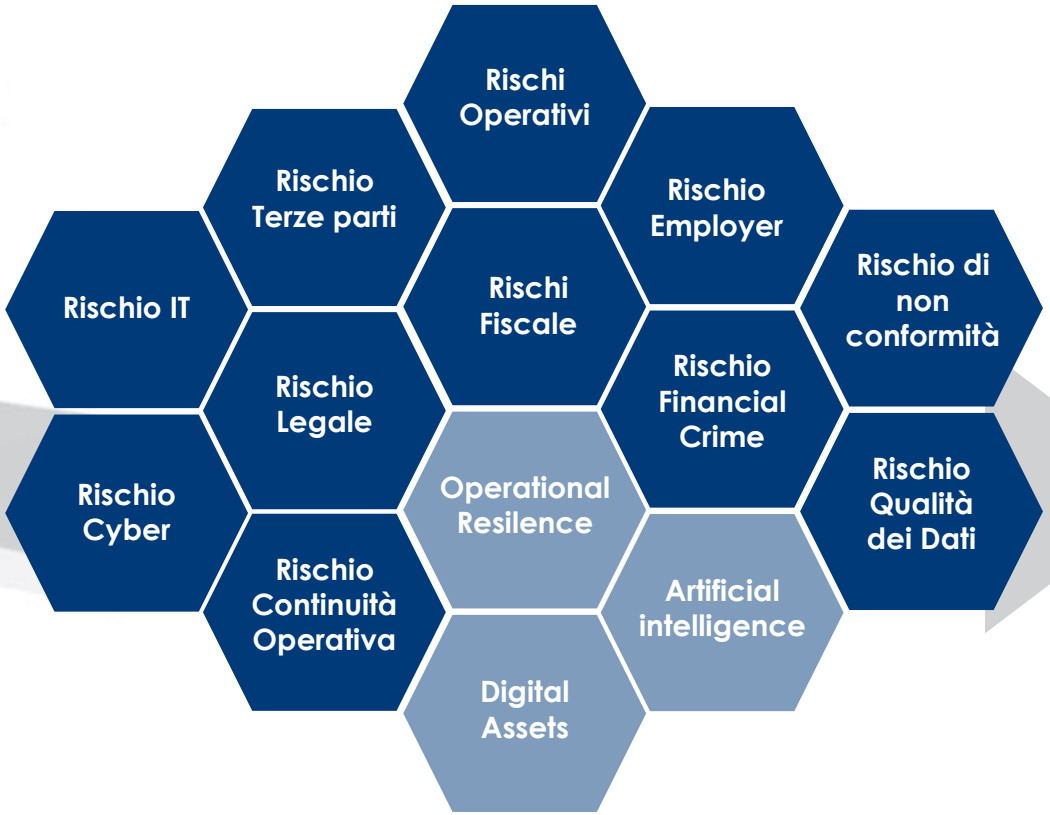
Nel corso degli ultimi anni la tassonomia dei rischi che rientrano nel più ampio perimetro dei rischi non finanziari si è molto arricchita, sia a seguito delle evoluzioni regolamentari che per esigenze gestionali

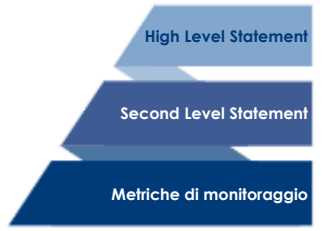
2015



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



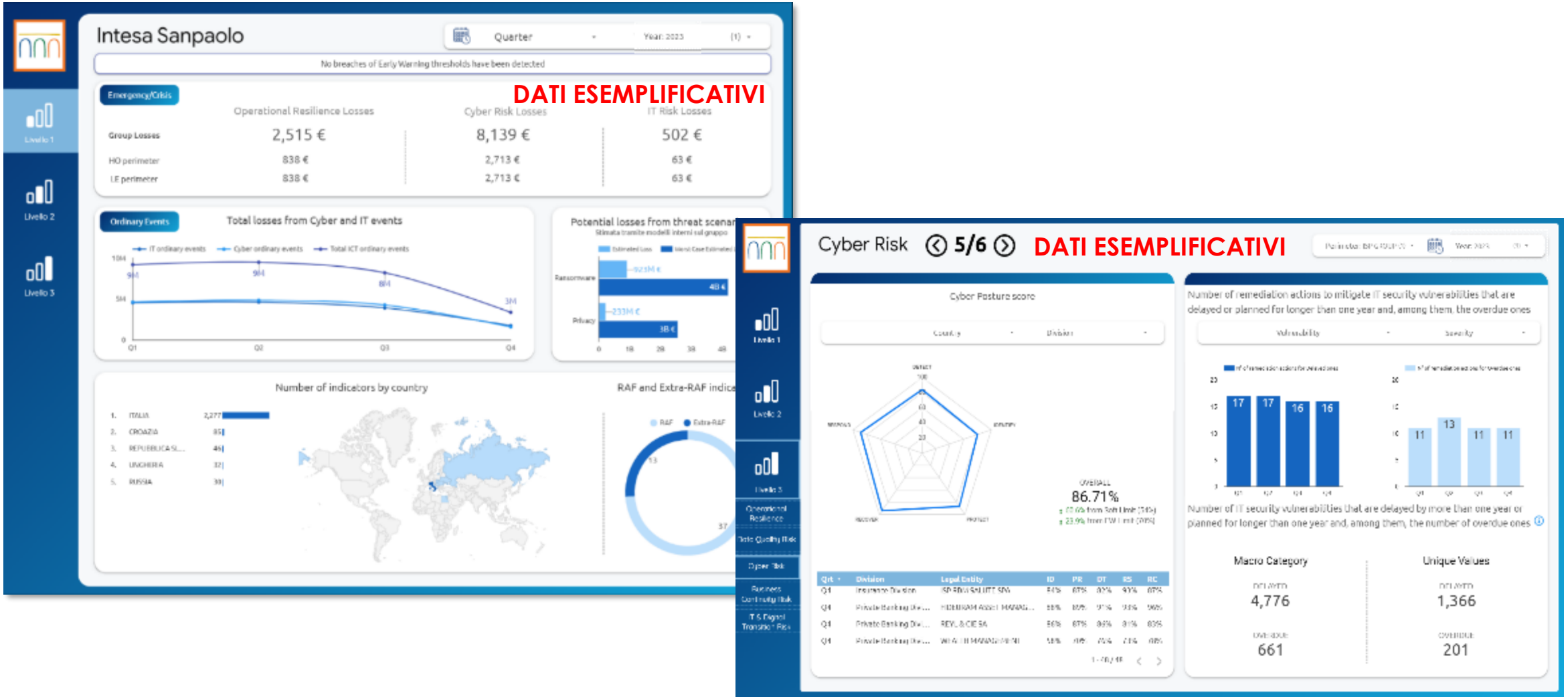


- **32 Metriche con limiti** (Early Warning, Soft Limit, Hard Limit)
- **34 indicatori**

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

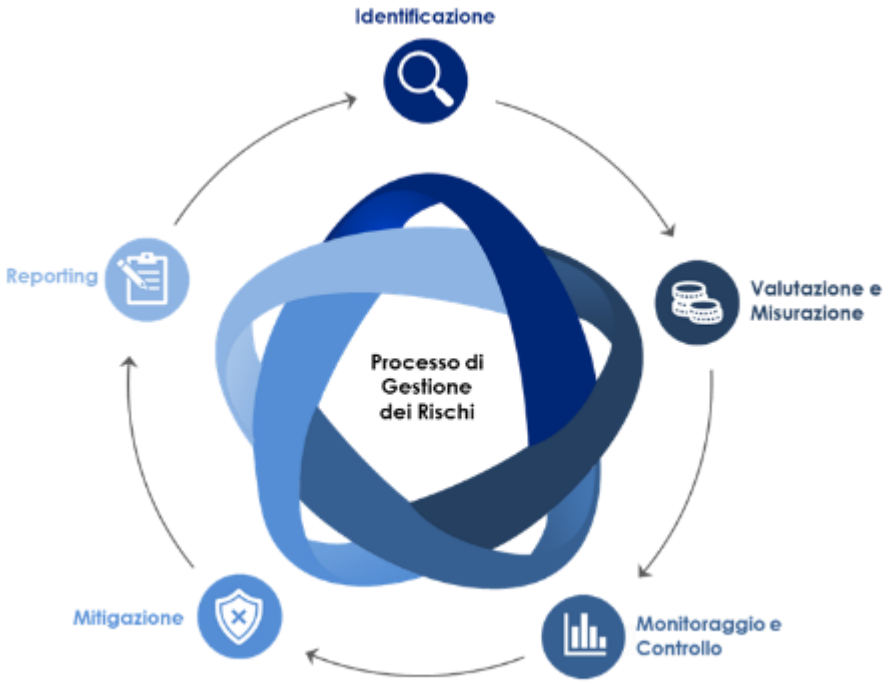
Per rafforzare il presidio della governance dei rischi non finanziari sono state introdotte delle dashboard di monitoraggio di metriche ed indicatori

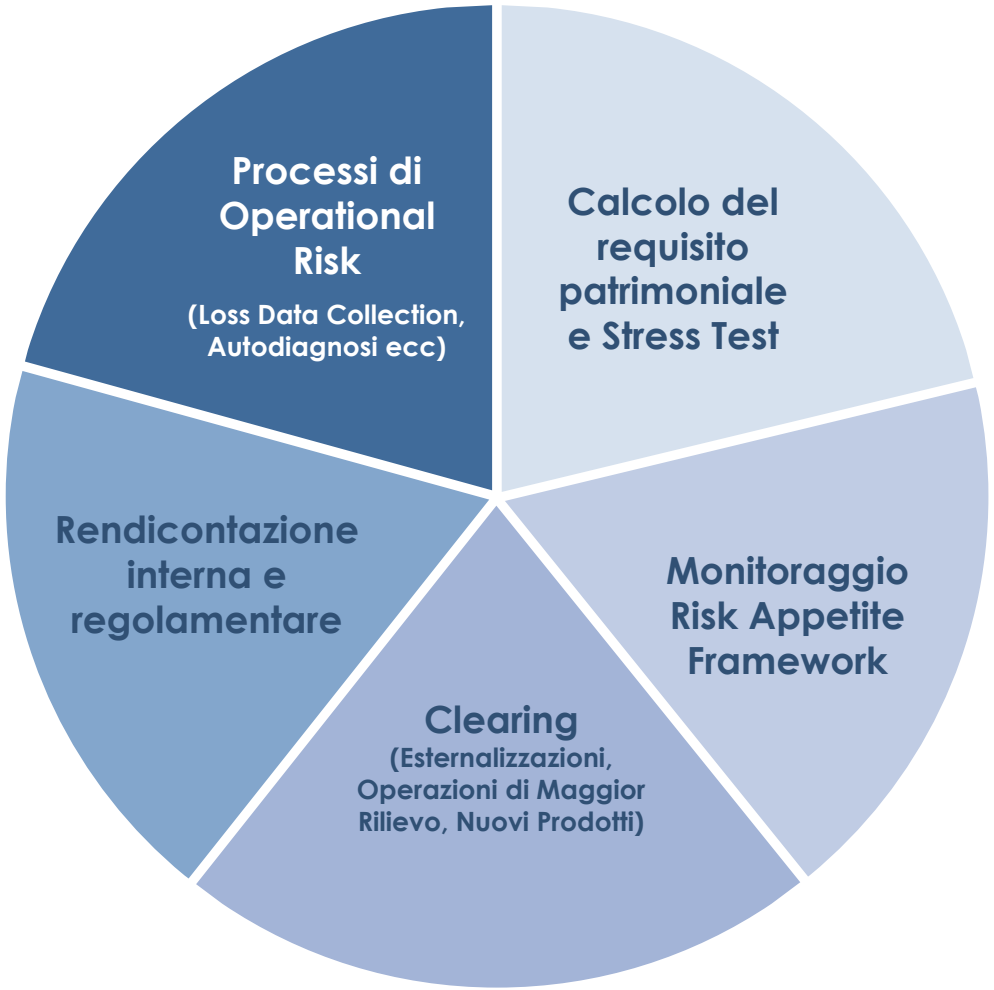
GOVERNANCE



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

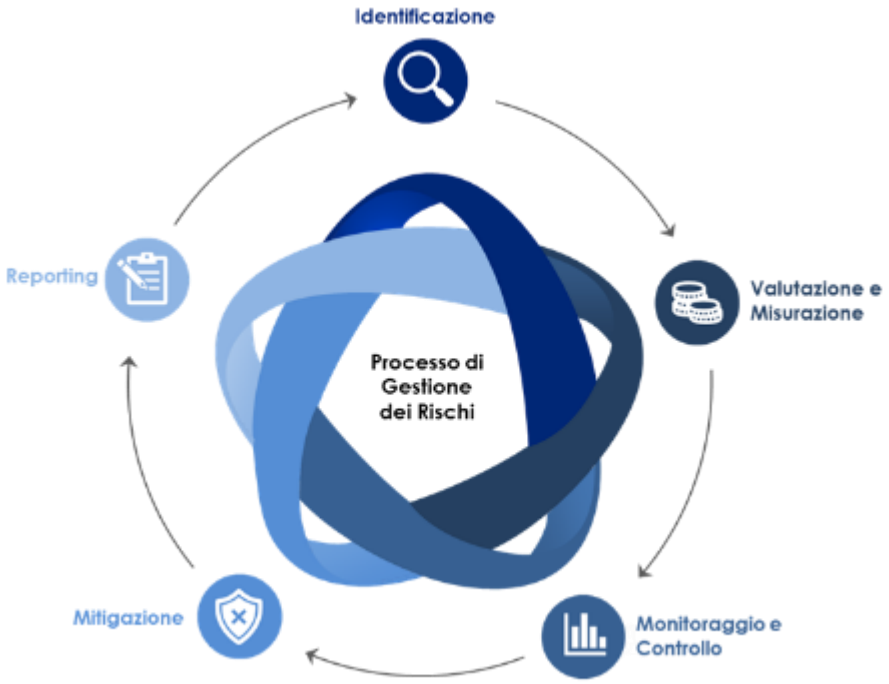
PROCESSES

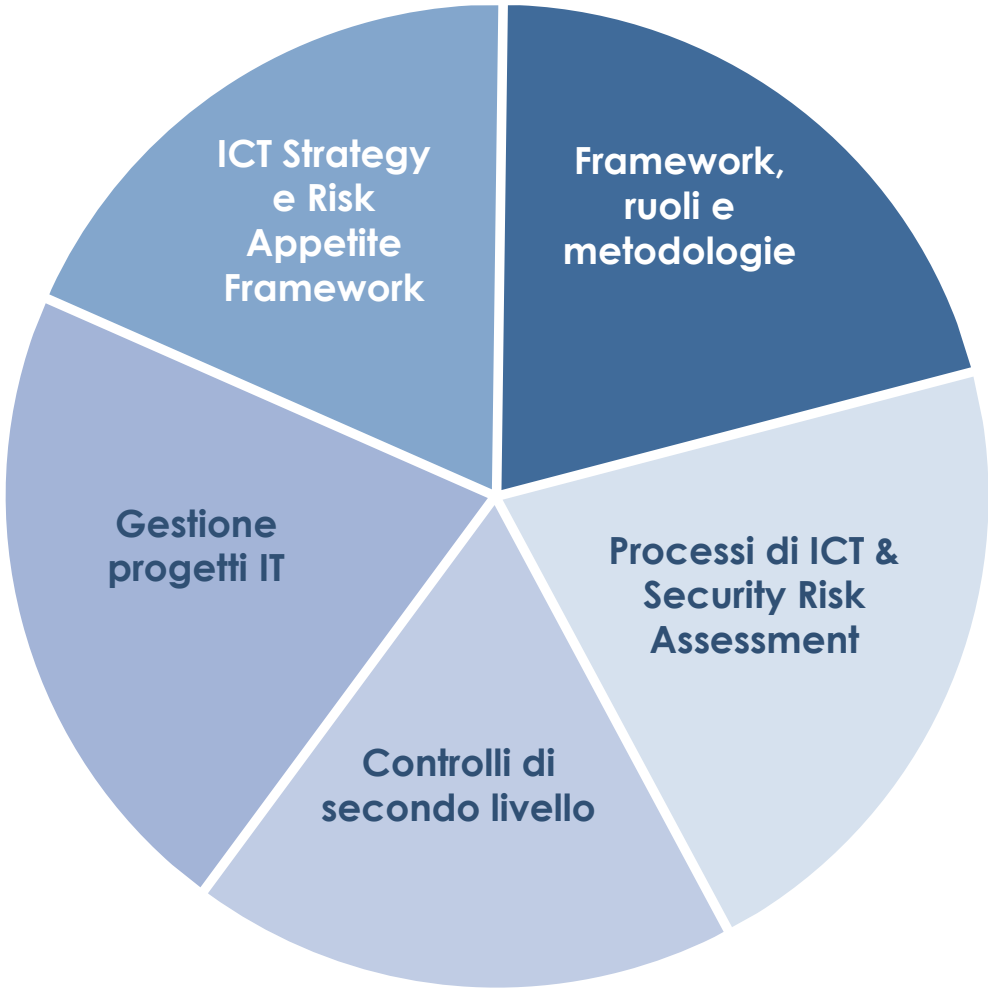




PROCESSES

… ICT e di Sicurezza





METHODOLOGY

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

Unknown-Knowns (fatti nascosti) ▪ Elementi non ancora noti ▪ Sconosciuti a noi, ma conosciuti ad altri	**Unknown-Unknowns** (rischi sconosciuti) ▪ Elementi non ancora noti ▪ Sconosciuti a noi e ad altri
Known-Knowns (fatti e requisiti) ▪ Non sono rischi ▪ Elementi gestiti come parte del perimetro di progetto	**Known-Unknowns** (rischi conosciuti) ▪ Rischi classicamente intesi ▪ Sono noti probabilità e impatto dei rischi

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….

INTESA SANPAOLO

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 organizzarti 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

INFRASTRUCTURE

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

DIGITAL CULTURE, SKILL & PROFESSIONS

SOUNDNESS ARCHITECTURE

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	Maggiore accuratezza modelli / controlli	Maggiore presidio dei rischi	Maggiore soddisfazione ed efficacia delle risorse
Medio - Alto	Alto	Alto	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

INFRASTRUCTURE

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

Piattaforma tecnologica cloud-based che abilita la creazione e l'utilizzo di **modelli statistici** e di **algoritmi** di **Data Science** e **Machine Learning**

Piattaforma analitica

Abilita utenti anche non esperti alla creazione **autonoma** di **reportistica** e **cruscotti** di sintesi con **strumenti visivi**

Self Reporting

Strumenti che facilitano l'**organizzazione** e la preparazione dei **dati** per le successive elaborazioni

Data Preparation

Gestione standard del **ciclo di vita** di **sviluppo** e **industrializzazione** dei **modelli** e aderenza agli **standard** di **Data Governance** e **Data Privacy**

Standard omogenei

Abilita gli **utenti** ad **analisi dati** autonome su modelli e algoritmi

Autonomia e collaborazione

Democratic Data Lab

Soluzione architetturale

Modello Operativo

Alimentazione dati consistente

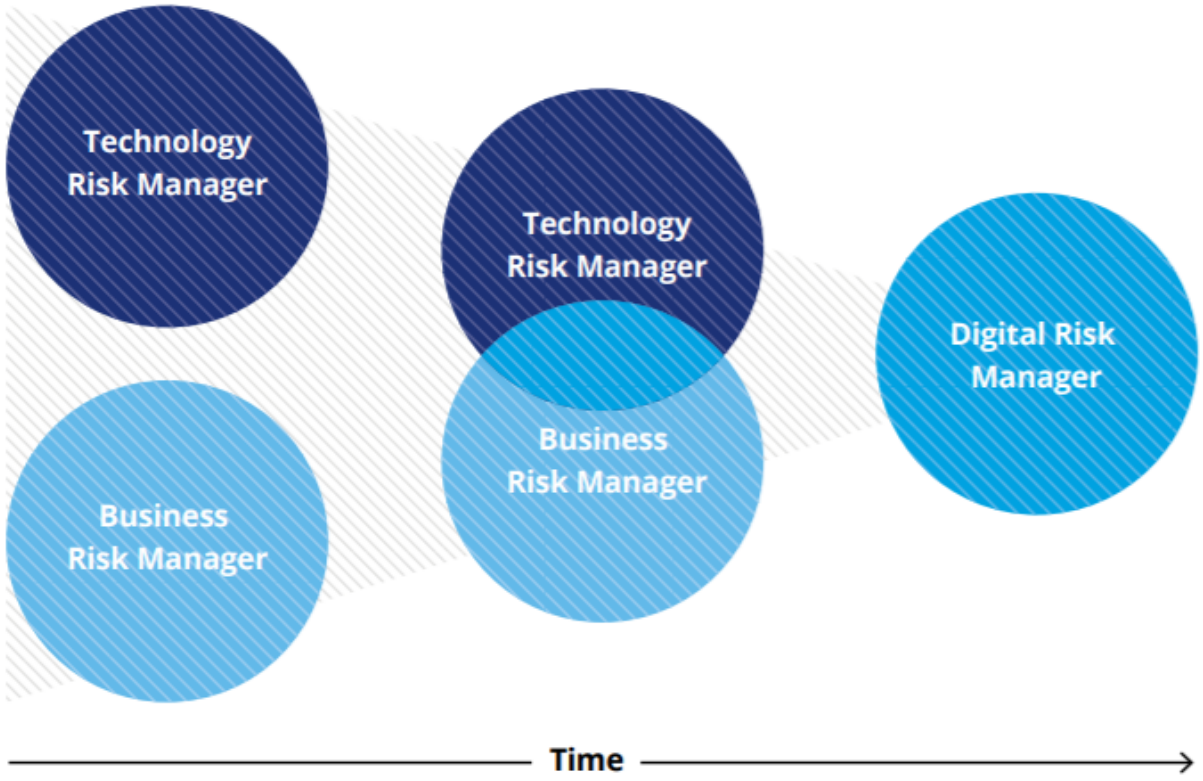
Alimentazione dati dal **Data Service Hub** aziendale

INTESA SANPAOLO

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	▪ **Allineamento nel continuo** con **Board** per tutte le fasi del processo (dalle Strategie operative alla mitigazione delle issues ed al piano dei trattamenti)
Digital & Data	▪ Definizione di una **strategia digitale complessiva** a livello di **Area CRO** ▪ **Introduzione** di logiche **data-driven** nei **processi** attuali, volte ad oggettivare le valutazioni dei self-assessment e costituire una base su cui implementare controlli di secondo livello ▪ Adozione di **strumenti analitici evoluti** (es. Democratic DataLabs) e **strumenti** di **monitoraggio**
Framework & Modelli	▪ Adozione logiche «**by design**» anche su controlli di primo livello, sicurezza e resilienza operativa ▪ Setup di un **framework** di **controllo** di **secondo livello** e messa a terra delle attività operative di controllo ▪ Adozione del **Risk Control Self Assessment** ▪ **Sviluppo** di **modelli** di **rischi non finanziari** forward-looking che puntano ad anticipare trend futuri e rischi emergenti (*unknown unknowns*) ▪ Evoluzione delle **metriche RAF** verso i **rischi emergenti** e più **rilevanti**
Persone	▪ Abilitare un **dialogo** «*streamless*» con le **funzioni tecniche** e **specialistiche** con «challenge» attivo ▪ Introduzione di nuove **figure professionali** ibride tra **Risk Manager** e **Technology Manager** ▪ **Rafforzare** le iniziative di **education** sui **contenuti specialistici** di **maggior rilevanza** per i **rischi emergenti**

… 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**