10 giugno 2026

Romina Vignotto, PwC Italia,
Partner

Oltre la frammentazione dei rischi operativi

Driver di rischio emergenti, prospettive di integrazione e generazione di valore strategico

Agenda

1. I Rischi Operativi: un ecosistema interconnesso la cui gestione genera valore strategico
2. Il contesto regolamentare
3. Il contesto operativo
4. Alcuni esempi di interconnessione fra rischi / driver di natura operativa: AI e Data Quality
5. Conclusioni: le leve di generazione del valore che derivano dal governo delle interconnessioni

I Rischi Operativi: un ecosistema interconnesso la cui gestione genera valore strategico

Governare la crescente interconnessione dei rischi operativi - eliminando le ridondanze di valutazione, valorizzandone le sinergie e dandone una rappresentazione unitaria agli Organi di Governo aziendale - consente di generare valore strategico sia in termini di *una più corretta valutazione e rappresentazione del rischio e del capitale* sia in termini di presidio, in ultima istanza, dell'*operational resilience*

Il contesto regolamentare

Il Rischio Operativo è qualificato nella regolamentazione di riferimento come il rischio di perdite derivanti da inadeguatezza o malfunzionamento di processi interni, persone e sistemi oppure da eventi esterni. Per sua natura si configura come categoria trasversale e complementare rispetto ai rischi finanziari, atta ad accogliere un novero particolarmente ampio di eventi che possono determinare esposizione al rischio stesso

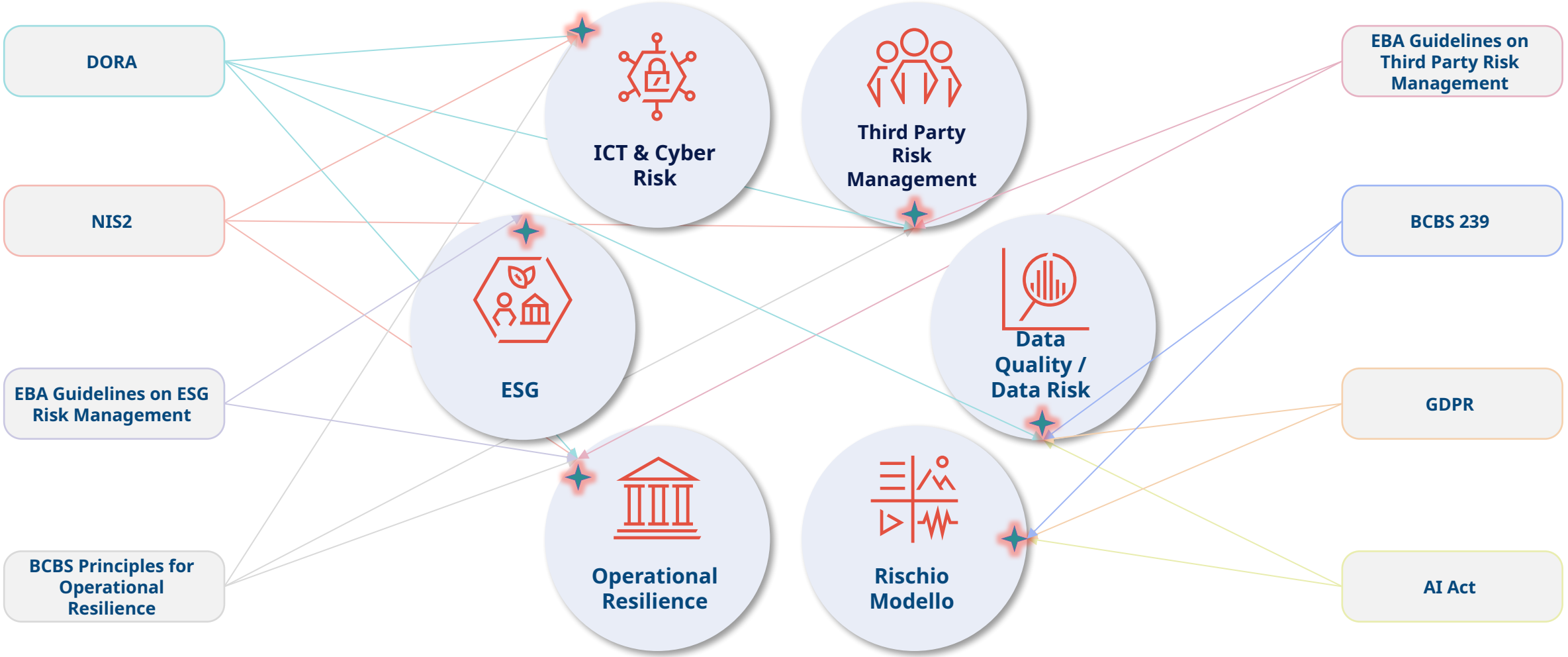
Il contesto operativo e le minacce che ne conseguono

L'evoluzione del contesto operativo ha generato diverse minacce e driver di rischio che incidono in maniera rilevante sull'esposizione al rischio operativo, quali ad esempio: le tensioni geo-politiche, i cambiamenti climatico ambientali, i gli attacchi di sicurezza informatica, la crescente dipendenza da fornitori esterni, l'innovazione tecnologica e il ricorso sempre maggiore all'intelligenza artificiale, la crescente dipendenza dai dati e dai modelli (anche generati da AI)

I rischi operativi come rischi interconnessi e non indipendenti fra di loro

La vera sfida nel contesto dei rischi operativi è quella di governare la crescente interconnessione fra le diverse fattispecie di rischio/driver di rischio che derivano dal contesto operativo e regolamentare, riconoscere la frammentazione che ne deriva per arrivare ad una visione olistica e non ridondante dell'esposizione ai rischi operativi stessi

Normative che si intersecano sui medesimi ambiti di rischio



Il contesto regolamentare è esso stesso **ricco, decisamente frammentato, nel contempo molto interconnesso in quanto punta al presidio di rischi che hanno impatto sui rischi operativi e/o dei medesimi driver di rischio che incidono su di essi**

Rischio / driver di rischio operativo al quale la normativa si riferisce

L'AI incide sui rischi operativi, attivando la Funzione preposta in coordinamento con altre Funzioni (presidio del rischio modello)

L'AI attiva contemporaneamente più rischi operativi...

È un **fattore di rischio trasversale** che incide su fattispecie di rischio già presenti nelle tassonomie

↓

Il **fattore di rischio è da analizzare in duplice veste**: quello derivante dallo sviluppo e adozione di modelli basati su AI; quello derivante da minacce esterne

↓

Pertanto, **attiva contemporaneamente** rischi tecnologici, rischi sul dato e sul modello, rischi di condotta e compliance

↓

È questa **simultaneità** che impone un **presidio integrato** e non verticale

...che si manifestano lungo tre macro-ambiti ricorrenti

Dati e Modelli

- Rischio Modello
- Rischio Protezione dei Dati

Tecnologie e Dipendenze

- Rischio IT
- Rischio Sicurezza Informatica
- Rischio Continuità Operativa
- Rischio Terze Parti

Compliance, Legale, Risorse Umane

- Rischio di Non Conformità
- Rischio Risorse Umane
- Rischio Condotta
- Rischio Legale

Il ruolo della Funzione di *Operational Risk*, in particolare per i modelli AI

Non sostituisce le Funzioni specialistiche, ma esercita un **challenge trasversale** sull'**intero** framework di gestione del rischio derivante da AI

1. Setting metodologico

Definisce i questionari di valutazione del rischio (in funzione delle caratteristiche del modello) e dei presidi a mitigazione

2. Risk opinion indipendente

Formula la risk opinion verso il Model Owner, l'AI Governance Pivot, gli altri attori del processo decisionale al momento dell'ideazione / sviluppo del modello

3. Monitoraggio e challenge

Esercita un ruolo di monitoraggio e challenge sui rischi identificati dalle Funzioni e sull'adeguatezza dei presidi messi in campo, post implementazione del modello

4. Vista unitaria

Rappresenta in sintesi il profilo di rischio derivante da AI verso gli Organi di Governo aziendale, in coordinamento con la Funzione che presidia il Model Risk

Il data quality risk è strettamente interconnesso con altre tipologie di rischio (operativi e non)

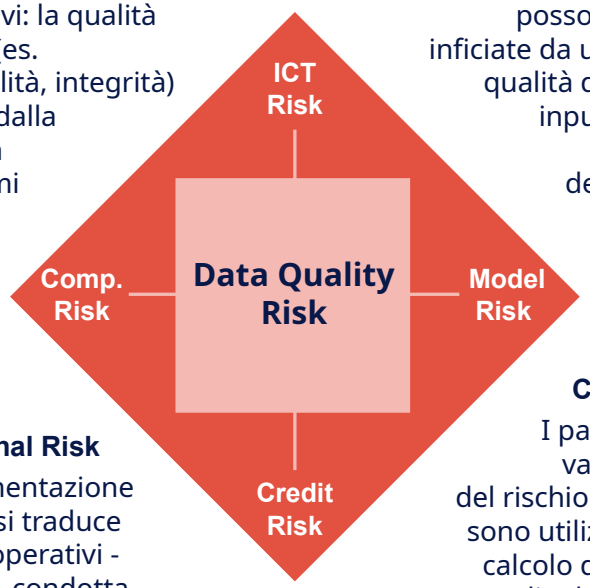
Il Data Quality Risk è esso stesso un rischio operativo ed è strettamente connesso con rischi presidiati da framework distinti…

ICT Risk

Il dato «nasce» e viene gestito da sistemi informativi: la qualità del dato (es. disponibilità, integrità) dipende dalla resilienza dei sistemi

Model Risk

Le decisioni assunte sulla base dei modelli possono essere inficiate da una scarsa qualità del dato in input al e/o in sviluppo del modello



Other Operational Risk

La frammentazione del dato si traduce in rischi operativi - processo, condotta, compliance - alimentati da decisioni su basi informative incoerenti

Credit Risk

I parametri di valutazione del rischio di credito sono utilizzati per il calcolo degli RWA: eventuali «*deficiencies*» di qualità del dato si traducono in add on (MOC A) di capitale

…generando delle potenziali aree di ridondanza

Valutazioni di rischio e capitale *double counted*

Metriche di rischio e capitale calcolate con perimetri e definizioni parzialmente sovrapposti

Duplicazione di controlli e di effort

Stesso dato verificato da più funzioni con logiche e metriche diverse

Ownership distribuita

Chi è responsabile della qualità del dato di perdita operativa?

Tassonomie incoerenti

Stessa dimensione di DQ definita in modo diverso tra framework

Reporting non riconciliato

Output verso il Supervisore e/o verso il Board basati su tassonomie differenti del dato

Il ruolo della Funzione di *Operational Risk*

Definire i confini del Data Quality Risk (come fattispecie di rischio operativo a sé stante o come driver di rischio)

Presidiare attivamente le aree di **sovrapposizione** con gli altri rischi

Restituire una **vista unitaria dell'esposizione** al rischio di qualità del dato

Come governare la crescente interconnessione dei rischi operativi?

L'interdipendenza fra rischi / driver di natura operativa è destinata ad aumentare. La risposta non è moltiplicare i presidi, ma ricomporli in una vista integrata e sinergica

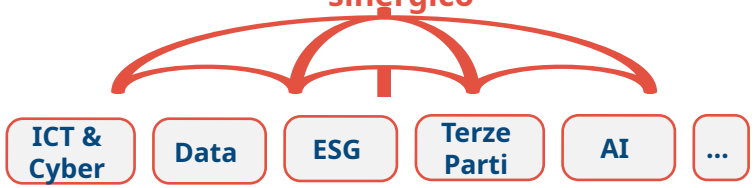
Oggi

Framework verticali in silos

- ICT & Cyber
- Data
- ESG
- Artificial Intelligence
- Terze Parti
- ...

Domani

Rischio Operativo come framework olistico e sinergico



E' opportuno pensare ad un'analisi strutturata dei framework di gestione dei rischi operativi che si sono tipicamente sviluppati «a silos», onde valutarne le aree di ridondanza e le aree di riconduzione ed efficientamento

Tassonomie comuni

Costruire un linguaggio condiviso tra rischi e funzioni: definizioni raccordate, eventi e cause di rischio ben delineate e raccordate con le fattispecie di rischio

Framework metodologico

Mappare ridondanze nelle metodologie di valutazione dei rischi operativi e le metriche su cui tali ridondanze si «scaricano» per intervenire a fini di razionalizzazione

Ownership e Governance

Definire responsabilità chiare ed evitare la dispersione dei presidi tra silos organizzativi, onde evitare duplicazioni di effort

Rappresentazione unitaria

Rappresentare agli Organi di Governo aziendale una sintesi coerente e raccordata del profilo di rischio non finanziario

La gestione unitaria del rischio operativo come leva di creazione di valore

Una gestione unitaria del rischio operativo consente da un lato di **evitare ridondanze nella valutazione del rischio e del capitale** ad esso connesso; dall'altro di **sostenere la resilienza operativa dell'Ente**, soprattutto laddove la valutazione unitaria dei rischi sia collegata ai «*critical business functions*» e orientata alla protezione dei servizi, attraverso l'identificazione dei punti di vulnerabilità operativa, delle interconnessioni fra rischi, delle catene causali e delle azioni a presidio

CONTATTI:

Romina Vignotto, Partner, PwC Italia
romina.vignotto@pwc.com