EVOLUZIONE NELL'ORGANIZZAZIONE AZIENDALE E NEGLI STRUMENTI DI CONTROLLO E MONITORAGGIO DEL RISCHIO

Sessione parallela F

17 maggio 2023

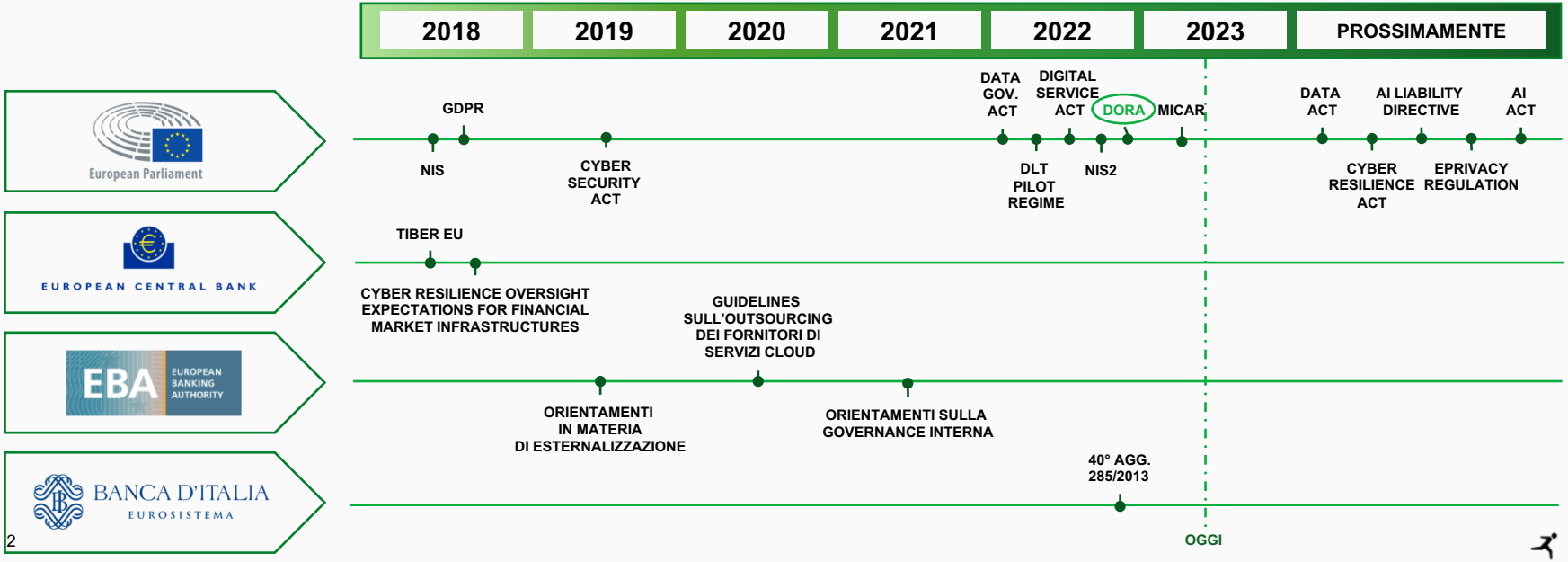
Paolo Fabris - Partner Avantage Reply

REPLY

L'EVOLUZIONE TECNOLOGICA HA RICHIESTO UN NUOVO FRAMEWORK REGOLAMENTARE...

L'evoluzione tecnologica degli ultimi anni ha generato **nuove sfide**: sicurezza in ambito ICT, governance, controllo, gestione e protezione dei dati sono temi sempre più presenti nelle agende degli istituti finanziari e dei regolatori.

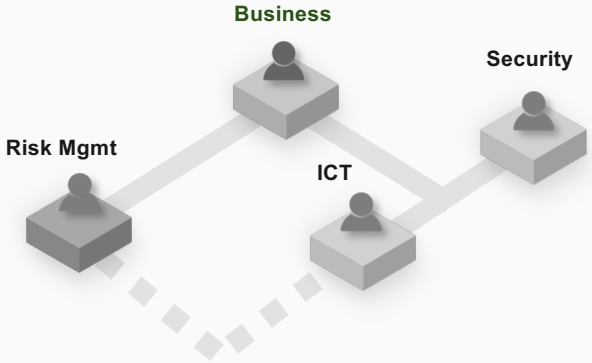
Altri eventi, come il COVID-19, hanno generato una rapida **accelerazione nella trasformazione digitale** (spinta della clientela vs canali digitali, nuove modalità di lavoro a distanza,…), aumentando l'attenzione della vigilanza e della politica rispetto alla nuova era dei rischi.



...E UN NUOVO PARADIGMA CULTURALE...

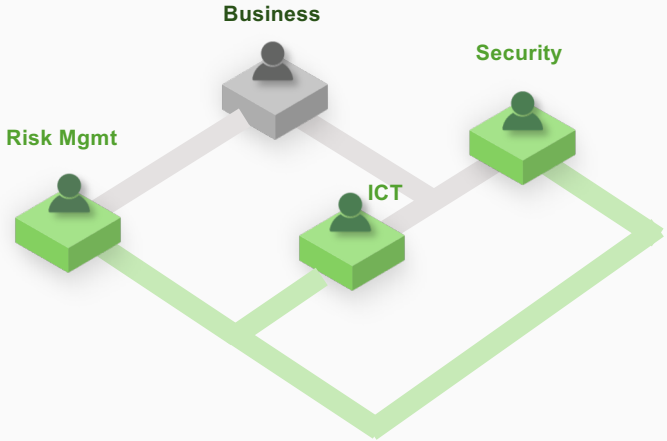
L'evoluzione tecnologica ha portato a un **nuovo paradigma culturale** anche all'interno del mondo finanziario con impatti sul modello organizzativo, sulla governance, sui processi e sui sistemi di controllo, concetto sottolineato anche dal nuovo Regolamento DORA.

ATTUALE PARADIGMA



- ICT e tecnologia come supporto al Business
- Sistema di controlli di sicurezza focalizzato alla gestione del Business
- Rischio ICT presente solo come fattispecie del rischio operativo
- Risk management come funzione di controllo di II Livello del Business

NUOVO PARADIGMA



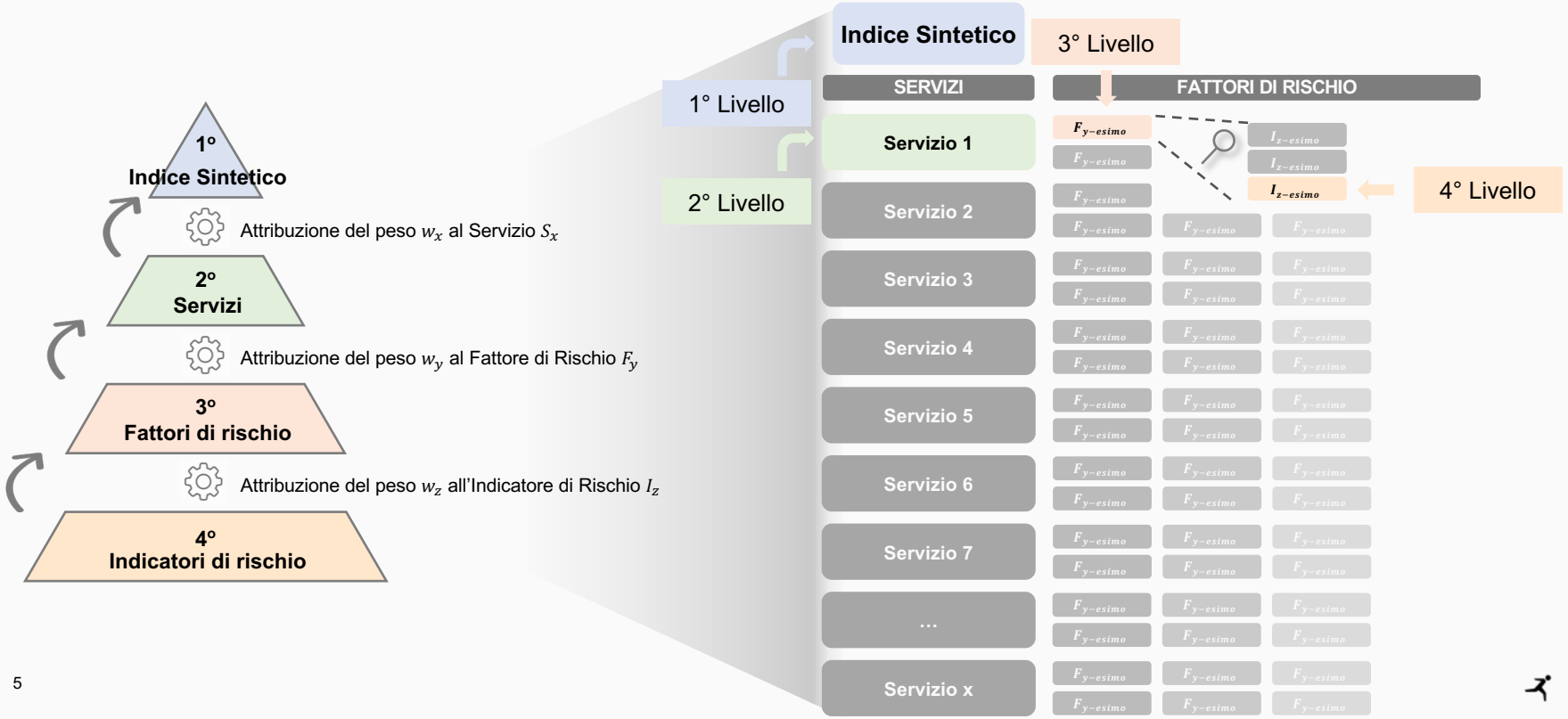
- ICT e tecnologia come asset strategico end-to-end
- Ampliamento del sistema di controlli di sicurezza anche a tutte le componenti ICT per una maggiore resilienza digitale
- Rischio ICT come componente autonoma di rischio
- **Risk management** come funzione di **controllo di II Livello** sia del **Business** sia di **ICT**, instaurando uno stretto dialogo anche con Security

...CHE RENDE NECESSARIO UN FRAMEWORK DEDICATO PER LA GESTIONE DEL RISCHIO ICT...

PERIMETRO	DATI	SOGLIE DI TOLLERANZA	TEST	MITIGAZIONE	MONITORAGGIO
					
• Mappatura funzioni e processi • Funzioni critiche o importanti • Interrelazioni	• Definizione metriche • Raccolta in un repository	• Definizione soglie di tolleranza • Risk Appetite Framework	• Definizione scenari di rischio • Esecuzione test	• Piano di remediation • Integrazione con framework Rischio Operativo	• Definizione di KPI e KRI • Creazione dashboard • Aggiornamento periodico del framework

...E IL RELATIVO MONITORAGGIO...

Per mantenere aggiornato l'intero framework è fondamentale disporre di **efficaci strumenti di monitoraggio** che consentano di tenere sotto controllo le principali metriche di rischio a diversi livelli di dettaglio informativo.



...PER AFFRONTARE IN SICUREZZA NUOVE SFIDE

DORA prevede l'incremento della cyber security e la sicurezza dei dati, soprattutto per i servizi sistemici.

SFIDE

- Espandere **perimetro** dei rischi
- Definire un **framework** end-to-end
- Implementare un modello di **monitoraggio**
- Sviluppare una nuova **BIA** basata su scenari significativi di discontinuità
- Sviluppare nuove metodologie di **test**
- Armonizzare la gestione dei **fornitori ICT**
- Sviluppare una **sensibilità** sulla dimensione **sistemica**
- Evolvere la **tassonomia** dei rischi ICT

OPPORTUNITÀ

- Rafforzare il livello di **sicurezza**
- Garantire maggior **presidio** dei rischi
- Sviluppare strumenti di **intelligence strategica**
- Ridurre i costi da **perdite operative**
- Mitigare il **rischio reputazionale**
- Ammodernare l'**architettura applicativa**
- Consolidare una visione **olistica** nell'ambito del **RAF**
- Integrare l'approccio nella gestione del **rischio operativo**