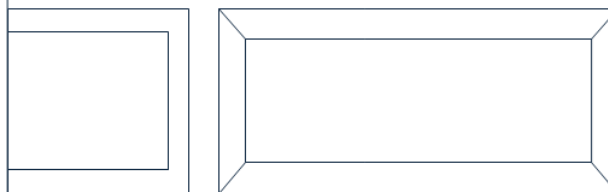


MEDIOBANCA GROUP IT EXECUTIVE SUMMARY

5 Maggio 2020



MEDIOBANCA

AGENDA

Introduzione

a) Mission

2.IT Gruppo Mediobanca

a) IT di Gruppo in sintesi

b) Modello di Governance

c) Mediobanca Innovation Services

3.Continuità operativa e Resilienza

4.Rischi IT & Cyber Security

5.Innovazione



MEDIOBANCA GROUP IT - MISSION

- ◆ Nel mondo dei servizi finanziari è in corso una profonda trasformazione dovuta all'**evoluzione delle tecnologie digitali** e al conseguente **cambiamento delle abitudini dei clienti**, fenomeno incentivato anche dal **mutato contesto competitivo**
- ◆ L'**IT** del Gruppo Mediobanca intende **realizzare una trasformazione interna** sfruttando le **nuove tecnologie** e guidando l'**evoluzione digitale**
- ◆ La **trasformazione interna** è funzionale a supportare:

i **clienti**
offrendo i
giusti prodotti
attraverso il
canale che
prediligono e
nel rispetto
dei requisiti di
sicurezza

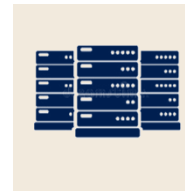


il **management**
agevolando le
decisioni con
l'ausilio delle
migliori soluzioni
tecnologiche

gli **azionisti**
offrendo un
vantaggio
rilevante nella
riduzione dei
costi e
aumentando
l'efficienza



i **dipendenti**
fornendo
strumenti che
supportano e
agevolano il
loro lavoro



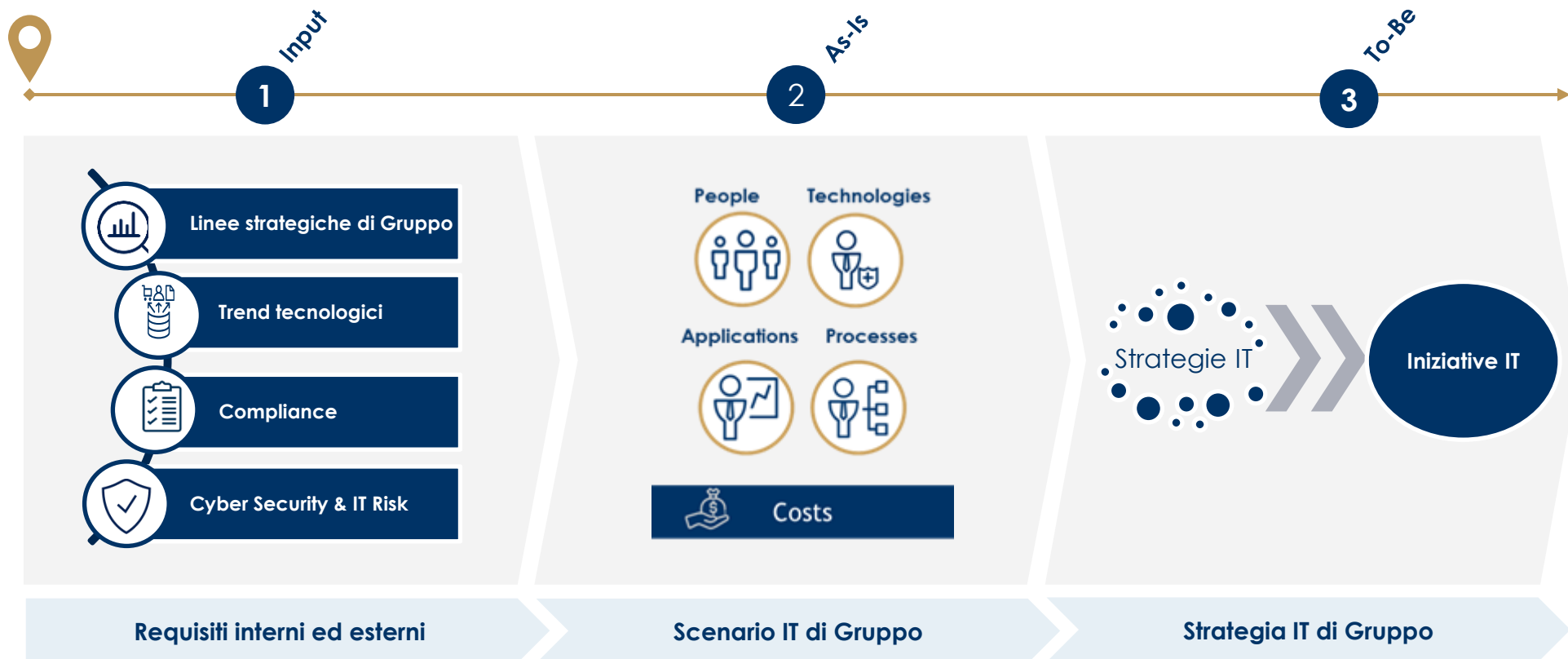
i **fornitori** per
mezzo di
strumenti
avanzati per la
collaborazione



le iniziative del
Gruppo
secondo i
criteri ESG

LA STRATEGIA IT SI CONCENTRA SULLE NECESSITÀ/OBIETTIVI DI GRUPPO...

La funzione IT è motore dell'evoluzione tecnologica e digitale a supporto degli obiettivi e delle necessità di business, con focus sulle priorità di medio/lungo termine al fine di promuovere un processo di sviluppo ordinato e coerente (sistemi, tecnologie e processi) verso un modello di banca "cognitiva" in grado di fornire a tutti gli utenti, clienti in primis, un'esperienza personalizzata.

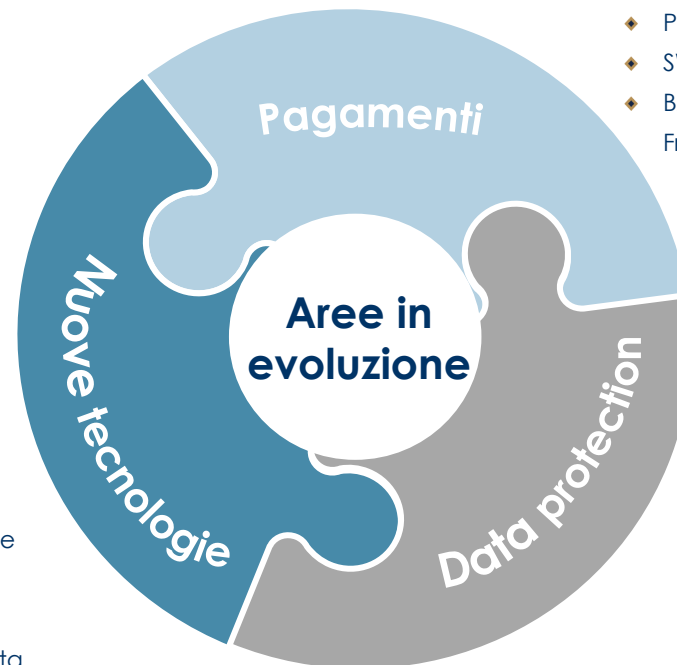


...E SULLA CRESCENTE REGOLAMENTAZIONE

- ◆ Il mondo bancario si confronta con continue **novità regolamentari** e ad esse è chiamato a rispondere. L'attenzione degli enti regolatori si concentra su alcune aree in continua evoluzione a causa dell'introduzione di **componenti tecnologiche innovative**
- ◆ Le normative (in vigore e in emanazione) evidenziano le implicazioni che i cambiamenti nella regolamentazione, nella gestione dei dati, nella digitalizzazione hanno e avranno sulla tecnologia bancaria



- ◆ EBA recommendations on outsourcing to cloud service providers
- ◆ Joint committee discussion paper on the use of Big Data by Financial Institutions



- ◆ PSD2
- ◆ SWIFT CSP
- ◆ BANCOMAT Security Verification Framework
 - ◆ MIFID II
 - ◆ IFRS 9
 - ◆ COREPc
- ◆ General Data Protection Regulation
- ◆ Article 29 Data Protection Working Party
- ◆ CBS 239

AGENDA

Introduzione

a) Mission

2.IT Gruppo Mediobanca

a) IT di Gruppo in sintesi

b) Modello di Governance

c) Mediobanca Innovation Services





3.Continuità operativa e Resilienza

4.Rischi IT & Cyber Security

5.Innovazione

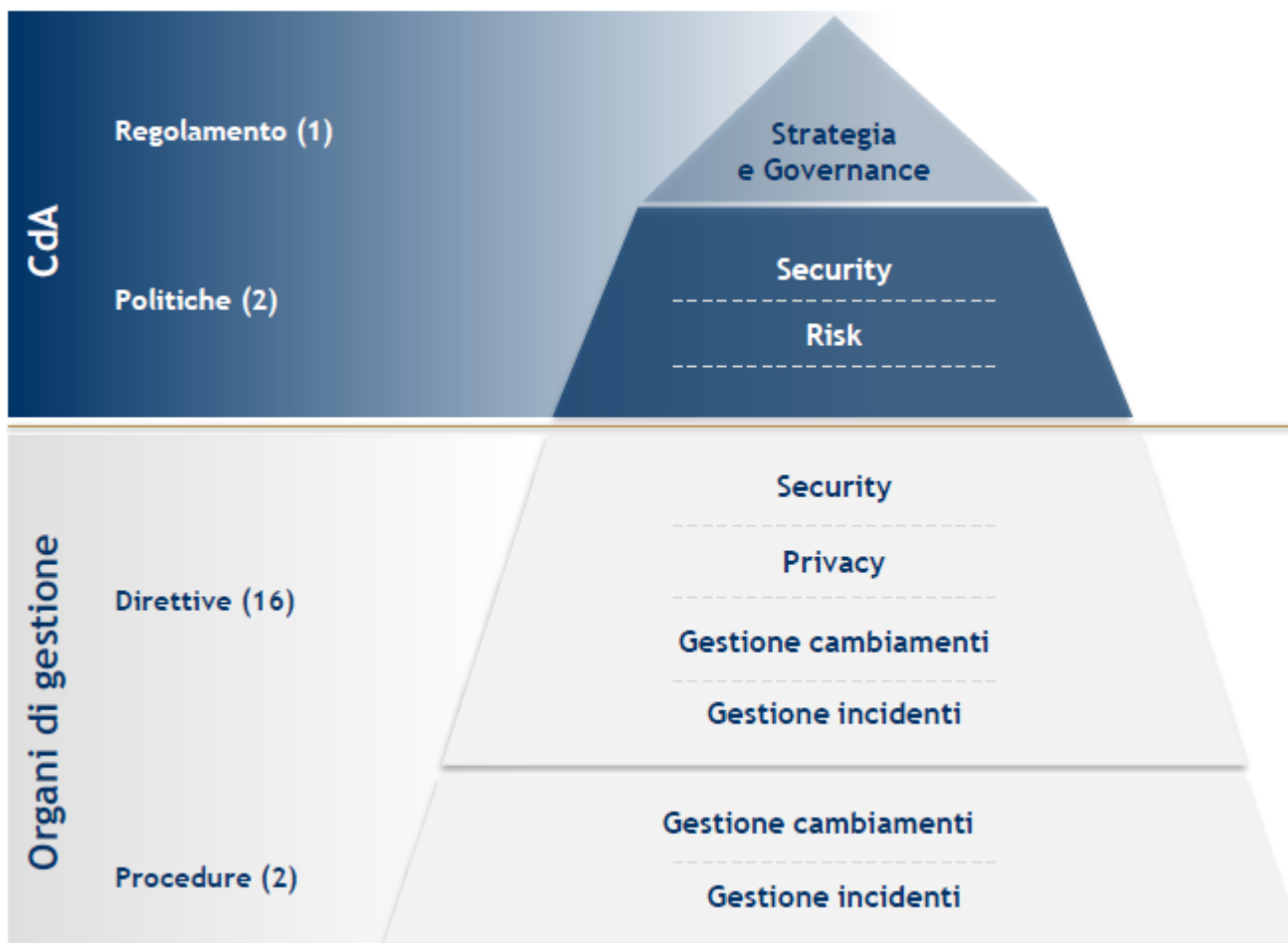


IT GRUPPO MEDIOBANCA IN SINTESI

Organico	Applicazioni	Tecnologia	Costi IT
<p>240 dipendenti IT</p> 	<p>750 Applicazioni di business</p> <p>300 Applicazioni «IT for IT»</p> 	<p>>3.700 server virtuali</p> <p>Ripartiti in un Data Center primario e un sito di DR</p> 	<p>187,8</p> <p>mIn Spesa IT nel FY18/19</p> 
<ul style="list-style-type: none">• 5% del totale organico di Gruppo• I dipendenti donne sono 1/5 dell'organico IT• Distribuzione per età migliore rispetto alla media del settore	<ul style="list-style-type: none">• Differenti approcci di gestione. Outsourcing delle funzioni <i>commodity</i>, gestione interna dei servizi <i>differenzianti per il business</i>• Elevata presenza di package di mercato (superiore alla media del settore)• Parco applicativo altamente specializzato coerentemente con le diverse necessità delle società del Gruppo	<ul style="list-style-type: none">• Asset tecnologici in carico alla società strumentale del gruppo MIS e gestiti in outsourcing da IBM• Investimenti in resilienza ed alta affidabilità dei data centers• In corso il piano di aggiornamento tecnologico per la sostituzione di alcune tecnologie non più all'avanguardia	<ul style="list-style-type: none">• I costi IT cregono dell'11% rispetto alla scorso FY in larga parte per l'ampliamento di perimetro (i.e consolidamento Banca Esperia) oltre che per lo sviluppo dell'attività bancaria (in particolare Consumer Banking e Specialty Finance)• gli investimenti IT aggiuntivi per l'avvio della rete promotori sono stati integralmente assorbiti dalle efficienze realizzate dall'integrazione del ramo d'azienda rilevato da Barclays

MODELLO DI GOVERNANCE DI GRUPPO

- ◆ Il **Gruppo Mediobanca** considera la **protezione delle informazioni** un principio primario per la salvaguardia e l'integrità del business e consente sia il raggiungimento di obiettivi strategici che il rispetto delle norme in vigore
- ◆ Il processo di gestione dei rischi IT è fondamentale per guidare il presidio organizzativo, procedurale e tecnologico e per verificare che le misure adottate siano appropriate all'entità dei rischi



Il regolamento IT di Gruppo descrive:

- il **modello di governance IT di Gruppo**;
- i **rispettivi ruoli e responsabilità** degli organi di governo ed unità organizzative coinvolte
- il ciclo di vita delle norme interne relative all'IT
- fa riferimento agli standard di mercato e alle migliori prassi, sia interne che esterne, su cui la Governance del Sistema Informativo di Gruppo si basa.

Mediobanca supervisiona il Sistema Informativo di Gruppo nell'interesse delle consociate, con l'obiettivo di promuovere l'adeguatezza del servizio a supporto del business, in ottica di sinergie e contenimento dei costi.

La gestione dell'infrastruttura tecnologica è centralizzata in Mediobanca Innovation Services, mentre la gestione del ciclo di vita delle singole specifiche applicazioni di business è affidato alle società del Gruppo.

MEDIOBANCA INNOVATION SERVICES (MIS)

Mediobanca Innovation Services (M.I.S.) è il centro di servizi ed innovazione tecnologica del Gruppo Mediobanca.

Garantisce l'erogazione dei servizi IT, di amministrazione e facility, supportando l'evoluzione dei sistemi informativi del Gruppo

AMMINISTRAZIONE E FACILITY

- ◆ Gestione Ciclo Attivo
- ◆ Gestione Ciclo Passivo
- ◆ Archiviazione Documentale
- ◆ Gestione Servizi Mobile
- ◆ Facility Management

APPLICATIVI

- ◆ Segnalazioni di Vigilanza
- ◆ Sistemi di Pagamento e Monetica
- ◆ Finanza
- ◆ Servizi di Tesoreria



TECHNICAL PARTNER

- ◆ Gestione della domanda tecnologica infrastrutturale
- ◆ Monitoraggio dei servizi erogati

ESTERNALIZZATO A IBM

- ◆ Storage e Backup
- ◆ Business Continuity
- ◆ Disaster Recovery
- ◆ Service Desk
- ◆ Gestione Rete (Voce e Dati)
- ◆ Change Management
- ◆ Informatica Individuale
- ◆ Sicurezza Operativa
- ◆ Servizi Sistemistici

AGENDA

Introduzione

a) Mission

2.IT Gruppo Mediobanca

a) IT di Gruppo in sintesi

b) Modello di Governance

c) Mediobanca Innovation Services

3.Continuità operativa e Resilienza

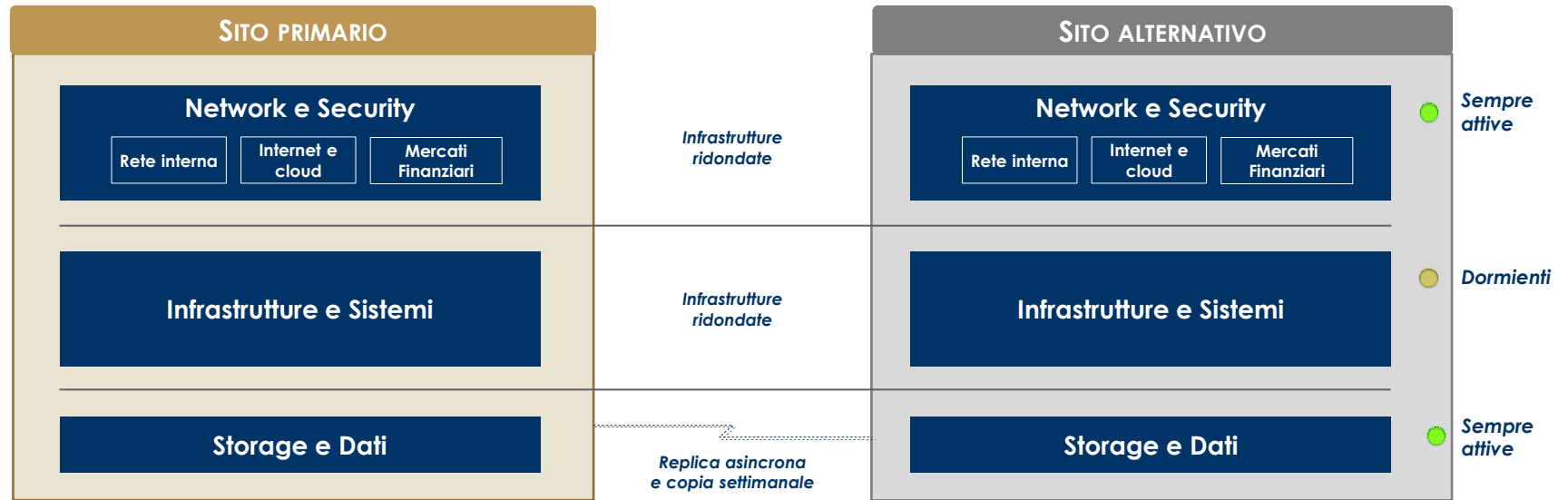
4.Rischi IT & Cyber Security

5.Innovazione



CONTINUITÀ OPERATIVA E RESILIENZA

L'**infrastruttura tecnologia di Gruppo** risiede nel sito primario di Via Siusi. Un sito alternativo (in configurazione active-passive) garantisce la **continuità** in caso di indisponibilità del data center primario (scenario di Disaster Recovery).



Investimenti in Resilienza e Alta Affidabilità

Mentre la soluzione di Disaster Recovery è pensata per proteggere l'operatività da eventi eccezionali (es. calamità naturali), gli investimenti in Alta Affidabilità sono volti a ridurre gli impatti di discontinuità di piccola entità, che possano verificarsi nel day-by-day a causa di errori umani e/o guasti ad apparati tecnici.

Fra le principali iniziative in questo ambito, si evidenziano:

- ◆ **il rafforzamento delle ridondanze di rete, storage e risorse di calcolo**, per ridurre ulteriormente il rischio di guasto
- ◆ **il potenziamento delle soluzioni di monitoraggio applicativo**, per una più tempestiva rilevazione dei malfunzionamenti
- ◆ **l'evoluzione dei processi di release management**, volta a minimizzare i rischi e a ridurre il time-to-market

AGENDA

Introduzione

a) Mission

2.IT Gruppo Mediobanca

a) IT di Gruppo in sintesi

b) Modello di Governance

c) Mediobanca Innovation Services

3.Continuità operativa e Resilienza

4.Rischi IT & Cyber Security

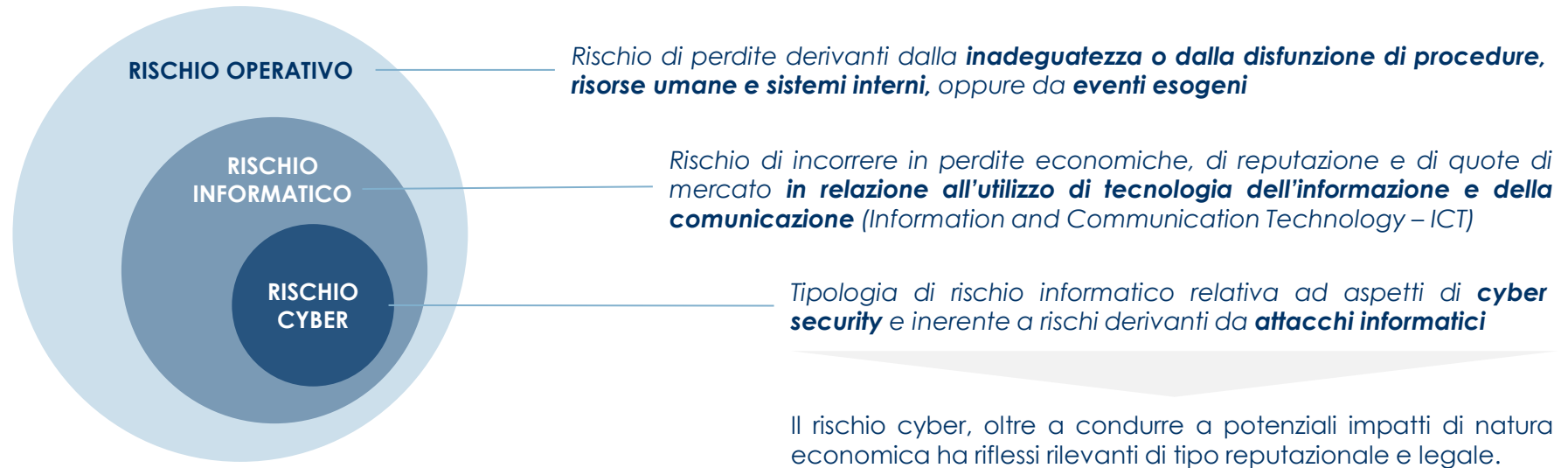
5.Innovazione



AMBITI DI RISCHIO IT

Il Gruppo Mediobanca, in accordo a quanto definito da Basilea, ha sviluppato un approccio integrato con il modello di gestione del rischio operativo per la gestione del Rischio informatico (comprensivo del Cyber Risk).

Contesto di riferimento



Gestione del Cyber Risk

- La gestione del rischio cyber prevede, oltre a misure di sicurezza di natura prettamente tecnologica, anche presidi di natura **organizzativa** e **procedurale** volti a **diffondere una cultura aziendale sulle tematiche di information security**
- Al fine di presidiare il cyber risk, Il Gruppo Mediobanca ha costituito la funzione di Gruppo '**IT Risk & Cyber Security**' all'interno di Group IT & Governance con riporto funzionale a **Operational Risk Management**

CYBER SECURITY STRATEGY DRIVER

Cyber Security Strategy Driver

La **strategia di sicurezza delle informazioni** è definita in relazione ad una serie di importanti **driver**.



PIANO INDUSTRIALE DEL GRUPPO

- ◆ Protezione adeguata del business delle Società acquisite (es. Esperia, RAM)
- ◆ Misure di sicurezza specifiche per nuove tipologie di Business (es. Wealth Management)



OBIETTIVI DI BUSINESS

- ◆ Misure di protezione differenziate in relazione allo specifico Business (corporate, retail, ecc)
- ◆ Garanzia del raggiungimento di un adeguato rapporto sicurezza/operatività



CONFORMITA' ALLE NORMATIVE

- ◆ Gestione delle misure di sicurezza previste dalle imminenti normative (GDPR, PSD2, EBA)



GESTIONE DEI RISCHI E DELLE FRODI

- ◆ Indirizzamento e gestione delle misure di mitigazione dei rischi e dei tentativi di frode
- ◆ Gestione di nuove minacce e tipologie di attacco informatico



EVOLUZIONE TECNOLOGICA

- ◆ Adozione di adeguate misure di sicurezza in linea con nuovi trend tecnologici e con l'evoluzione digitale soprattutto in relazione al settore retail banking



GESTIONE DEGLI INCIDENTI

- ◆ Garanzia della resilienza del Business a fronte del verificarsi di incidenti
- ◆ Apprendimento dagli incidenti (lesson learned) e definizione delle misure di prevenzione

IT RISK & CYBER SECURITY FRAMEWORK

La declinazione della strategia di Cyber Security avviene tramite la definizione del '**IT Risk & Cyber Security Framework**', ovvero di un modello di riferimento per la gestione di attività di carattere tecnologico, procedurale e organizzativo volte alla protezione del patrimonio informativo del Gruppo.

FRAMEWORK	IDENTIFICARE	PROTEGGERE	INDIVIDUARE	REAGIRE
	Approccio 'Proattivo'	Approccio 'Proattivo'	Approccio 'Investigativo'	Approccio 'Reattivo'
	Comprensione del contesto di business , degli asset che supportano le funzioni critiche e i relativi rischi IT.	Limitare gli impatti di un potenziale incidente gestendo identità e accesso, protezione dei dati, formazione, procedure e processi di sicurezza.	Attività volte all' identificazione di eventi di rischio che possono compromettere la protezione del patrimonio informativo	Attività volte alla gestione di eventi / incidenti e al ripristino dell'operatività limitando gli impatti sul Business (resilienza)
	• Information Security management System	• Standard architetturali di sicurezza	• Disegno controlli e analisi eventi	• Cyber Security defence plan
	• Gestione degli asset	• Protezione identità e controllo degli accessi	• Servizi di Security Continuous Monitoring	• Gestione delle frodi finanziarie
	• Missione della funzione Cyber Security	• Risk and Security awareness	• Monitoraggio Outsourcing Risk	• Gestione relazione con SOC
• Analisi e valutazione dei rischi IT	• Sicurezza dei dati	• Security Testing	• Certfin e knowledge sharing	
• Strategia IT Risk	• Procedure per la sicurezza operativa	• Analisi evoluzione scenari di attacco	• Centro di competenza gestione incidenti di Sicurezza	

Caratteristiche del Framework:

- ✓ Il framework è indipendente dalle tecnologie, si ispira a best practice e standard di settore (NIST, 27001) e riflette le Direttive emanate dal Gruppo Mediobanca.*
- ✓ Il framework usa un approccio risk based per indirizzare le priorità e qualificare le decisioni che il Gruppo dovrà intraprendere
- ✓ Il framework garantisce scalabilità e flessibilità, ovvero si pone l'obiettivo di evolvere in accordo con le variazioni dei modelli e canali di business delle Società e con l'evoluzione degli attacchi e dei nuovi trend tecnologici o architetturali.
- ✓ Il framework promuove un paradigma di Cyber security e IT Risk 'proattivo' stressando il concetto di «detection» di attacchi e la gestione 'by design' delle debolezze che possono essere sfruttate per perpetrare frodi finanziarie e attacchi informatici.

IT RISK & CYBER SECURITY – APPROCCI

PREVENTION

Sviluppare un'organizzazione orientata al cyber security risk al fine di proteggere le infrastrutture critiche, le risorse umane e i dati critici per il business.

Information Security System

- Garanzia di protezione in termini di **riservatezza** e **integrità** del patrimonio informativo del Gruppo

Standard architetturali di Sicurezza

- Servizi tecnologici secondo un approccio '**Security by Design**'

Risk and Security Awareness

- **Formazione e sensibilizzazione** su tematiche di Information Security

Controlli e misure di Sicurezza

- Definizione dei **controlli di sicurezza** per mezzo di **Competenze - Modelli di Business - Modelli operativi**

DETECTION

Coinvolgimento in tutte le fasi del ciclo di vita di un servizio, garantendo un monitoraggio puntuale del rischio e delle minacce al fine di governare la sicurezza e protezione delle informazioni del Gruppo.

Analisi del rischio

- Per assicurare l'efficacia delle misure di protezione delle risorse ICT

Monitoraggio outsourcing risk

- Monitoraggio e governo dei rischi IT legati all'outsourcing

Security Testing

- Verifica livello di sicurezza dei sistemi che trattano dati e servizi critici

Analisi scenari di rischio

- Quantificazione soggettiva del rischio, supportata da parametri quantitativi

Evoluzione scenari di rischio

- Analisi di nuove metodologie per mantenere adeguati livelli di protezione

REACTION

- **Sviluppare una risposta ordinata** a livello Corporate che guida le azioni da intraprendere in risposta ad un attacco - **Cyber Security Defense Plan**
- Definire i piani di resilienza per **limitare gli impatti di un attacco di Sicurezza**
- Implementare piani operativi per **il ripristino dei servizi e l'accesso alle informazioni**

Cyber Security Defense Plan

- Definizione di un piano di risposta agli incidenti di sicurezza volto a mitigare un attacco sin dalle prime fasi

Enterprise Fraud Management

- Supporto alle società del Gruppo nella rilevazione delle frodi finanziarie

Security Operation Center

- Garantisce una pronta risposta in caso si verificano incidenti di sicurezza

Knowledge Sharing

- Partecipazione a CERTFin, cooperazione finalizzata a innalzare la capacità di gestione dei rischi cyber

AGENDA

Introduzione

a) Mission

2.IT Gruppo Mediobanca

a) IT di Gruppo in sintesi

b) Modello di Governance

c) Mediobanca Innovation Services

3.Continuità operativa e Resilienza

4.Rischi IT & Cyber Security

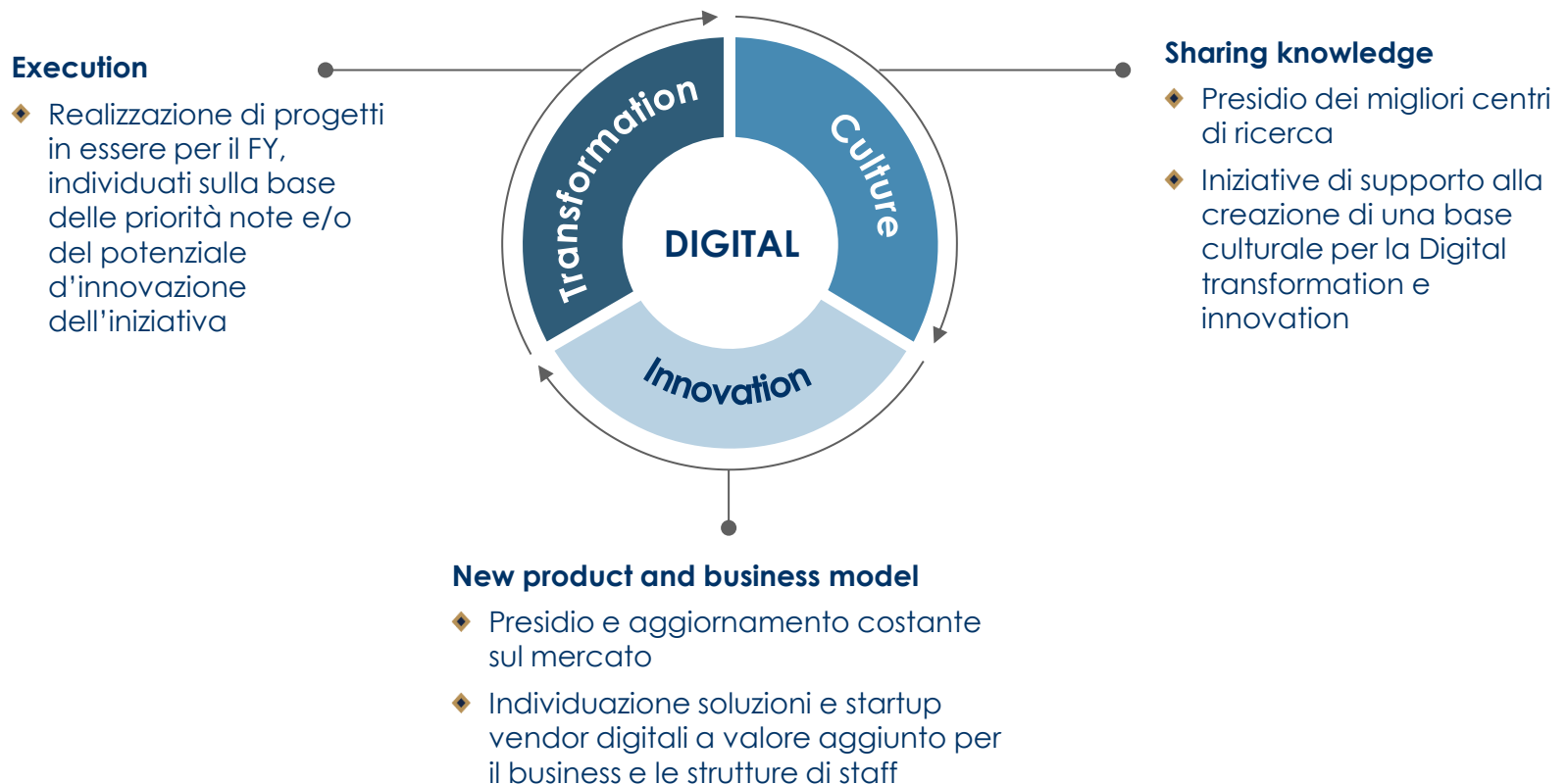
5.Innovazione



INNOVAZIONE

Mission Pillars

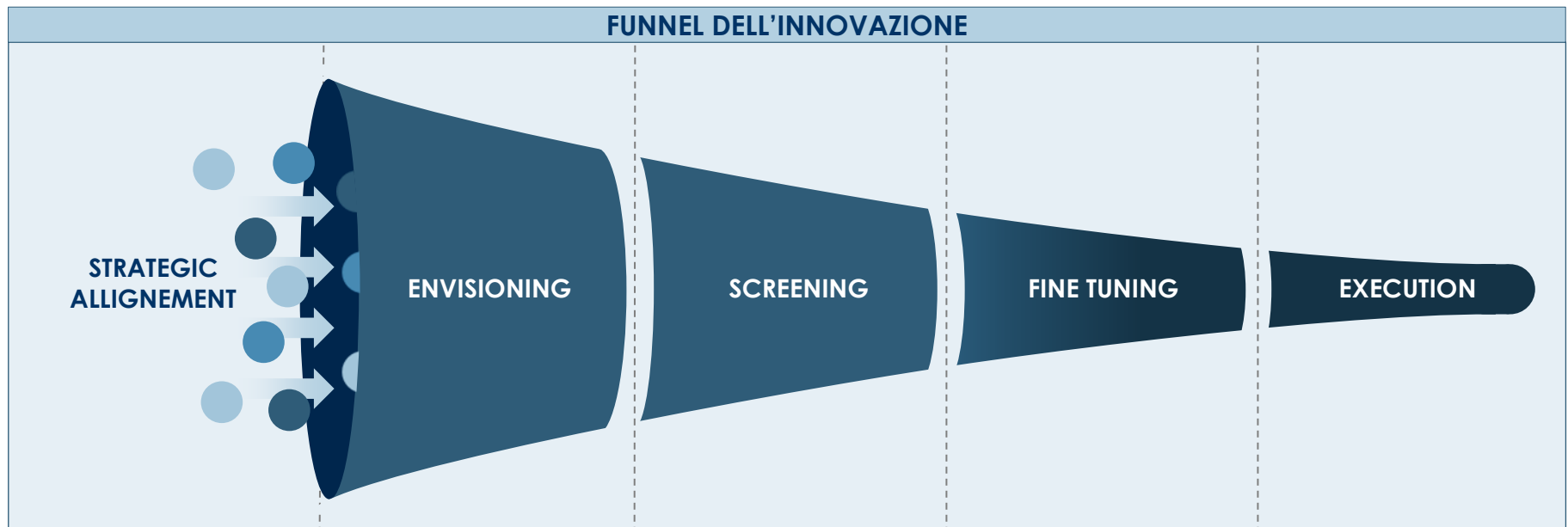
- ◆ All'interno dei piani di sviluppo di Mediobanca uno degli obiettivi strategici è quello **presidiare e stimolare i diversi aspetti connessi all'innovazione digitale del Gruppo**
- ◆ Nell'ambito del Gruppo oggi le tematiche legate all'innovazione si basano sui **pillar principali: Digital Business Transformation, Culture e Innovation**



INNOVAZIONE

Il funnel

- ◆ Al fine di favorire l'introduzione e lo sviluppo di nuove tecnologie in Mediobanca l'unità IT Strategy and Digital Innovation presidia un **processo sistematico di innovazione** che coniuga gli stimoli esterni raccolti con la partecipazione ad iniziative di mercato, collaborazione con **Fintech e Centri di ricerca**, ascolta le esigenze provenienti dal Gruppo e declina una **roadmap pragmatica** di priorità in linea con gli obiettivi strategici delle divisioni business.ì

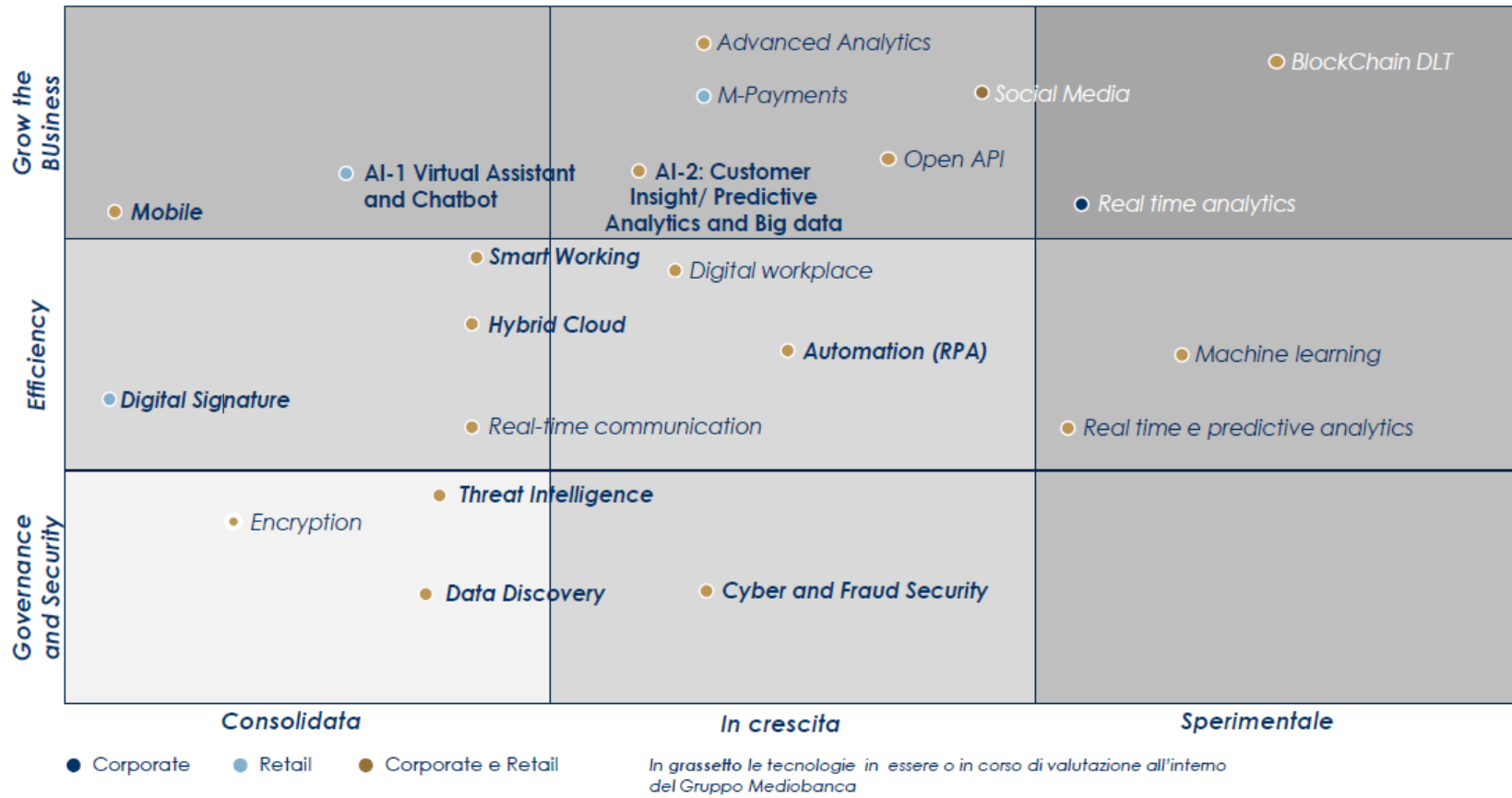


- ◆ Dall'allineamento strategico all'execution le idee vengono raccolte attraverso ascolto interno ed esterno e via via selezionate in base alla coerenza con le priorità strategiche e in ottica di individuazione della migliore opportunità

INNOVAZIONE

Nuove tecnologie

- ◆ L'unità di innovazione, nell'ambito della **Strategia Digitale**, monitora in maniera continuativa le nuove tecnologie per valutare l'opportunità di una eventuale adozione rispetto al grado di maturità della tecnologia stessa



INNOVAZIONE

Progetti e sperimentazioni

Nell'ambito del Gruppo sono state create unità organizzative, gruppi di lavoro e partnership volte a promuovere la diffusione dell'innovazione (anche dal punto di vista divulgativo), il che ci consente di avere una posizione di rilievo sulla frontiera tecnologica.



MEDIOBANCA

All'interno della Direzione COO IT Strategy and Digital Innovation è l'unità organizzativa dedicata allo studio e alla sperimentazione delle nuove tecnologie



EUROPEAN
FINANCIAL
TRANSPARENCY
GATEWAY



Progetto che sfrutta tecnologia blockchain per la gestione delle informazioni regolamentate europee



Progetto Spunta interbancaria, Partnership con la Fintech R3 (piattaforma Corda) in collaborazione con ABILAB



Chat

Progetto Chatbot – Assistente virtuale realizzato in CheBanca! capace di conversare in linguaggio naturale con i clienti



Approccio Test & Learn per applicazioni AI in ambito Private Banking e CIB