INTESA SANPAOLO
GROUP SERVICES

# La consapevolezza del rischio come base per il Governo della Sicurezza di Gruppo

Alberto Sferch
Responsabile Governo Sicurezza e Continuità Operativa

**Banche e Sicurezza 2014**

Milano, 27 Maggio 2014

**Il contesto legislativo**

Il contesto di business e operativo

L'evoluzione degli scenari

L'approccio basato sul rischio

Alcuni spunti di riflessione

# L'evoluzione del contesto legislativo in Europa e in Italia


Nel corso degli ultimi anni il sistema bancario, ed in particolare Intesa Sanpaolo in quanto banca di rilevanza sistemica, è stato oggetto di numerosi interventi normativi aventi l'obiettivo di:

- **garantire la continuità** della banca in caso di **incidente o crisi** (operative, finanziarie e di liquidità)
- **proteggere il cliente** a fronte dell'erogazione di servizi mediante canali innovativi e ad alto contenuto tecnologico
- **integrare** i rischi tecnologici e di continuità operativa **nel sistema dei controlli della banca**

# Il nuovo quadro normativo richiede strumenti aggiornati per la Governance di Sicurezza

L'evoluzione del contesto normativo italiano ed europeo comporta la necessità che la banca affini il proprio ruolo di Capogruppo per governare le diverse **etoregeneità presenti nel Gruppo** mediante **sistemi e strumenti di armonizzazione** idonei a fornire i **livelli di protezione** richiesti dalla normativa

## Requisiti Normativi

- Comprensione dei livelli di rischio
- Policy, strumenti, processi e controlli di Sicurezza IT e di Business Continuity
- Piena consapevolezza degli organi aziendali

*Eterogeneità*

| nel contesto territoriale | nelle entità di Gruppo | nelle cultura del rischio della banca |
|---|---|---|
| (richieste dei regolatori locali non sempre uniformate a quelle del regolatore centrale) | (banche e società prodotto con dimensioni, processi e volumi diversi) | (inserimento del rischio IT nel "rischio banca" focalizzato sulla tassonomia classica: rischi operativi, di mercato, di liquidità) |

*Armonizzazione*

| soluzioni centrali e locali | nuovi sistemi di Governance | unica strategia di rischio (RAF) |
|---|---|---|
| indirizzo centralizzato dei requisiti richiesti sia da Banca d'Italia sia dalle Banche Centrali locali | per il controllo diretto, o indiretto, sulle diverse entità del Gruppo | (integrazione del Rischio IT e della Continuità Operativa nel Sistema aziendale di Governo del Rischio) |

- Il contesto legislativo
- **Il contesto di business e operativo**
- L'evoluzione degli scenari
- L'approccio basato sul rischio
- Alcuni spunti di riflessione

# L'evoluzione del Business bancario

Le mutate condizioni economiche degli ultimi anni e l'evoluzione del sistema bancario determinano la **modifica del modello** di **business** e **operativo** della banca con significativi impatti sulla **riorganizzazione delle competenze** e sull'**ottimizzazione degli investimenti**

| BUSINESS | | COO | |
|---|---|---|---|
| **Nuovi prodotti e servizi** | **Customer satisfaction** | **Agility** | **Tecnologia abilitante** |
| Sviluppo di prodotti ad alto contenuto tecnologico a supporto dei canali diretti | Sviluppo di nuove competenze e professionalità per fornire servizi di maggior qualità | Ridisegno delle strutture organizzative e dei modelli operativi per ridurre i costi e incrementare l'efficienza della macchina operativa | Sviluppo di piattaforme IT a supporto del business e coerenti con i vincoli di time-to-market del settore<br>Adozione di nuove tecnologie per incrementare l'efficienza dei processi interni (es. dematerializzazione, digitalizzazione,...) |

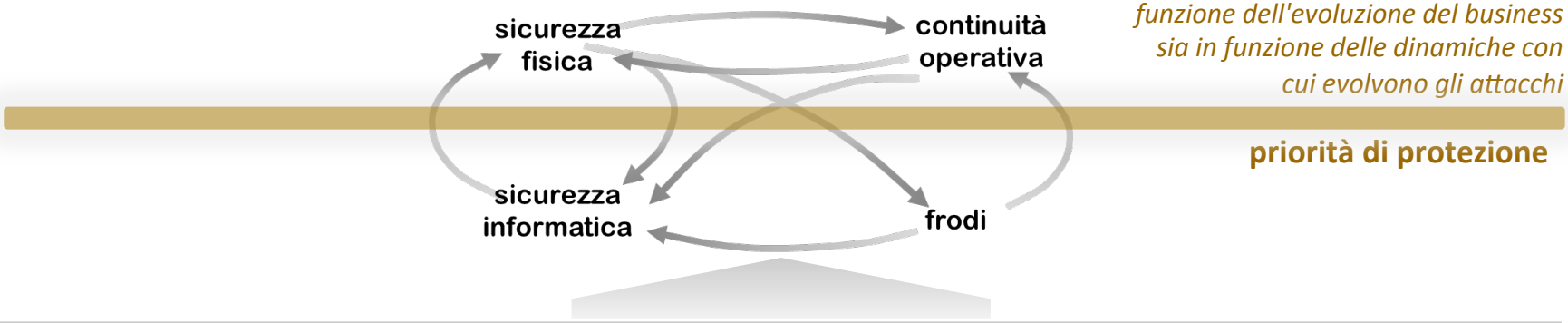
**Priorità di protezione**

*le esigenze di efficienza e velocità di adattamento al contesto esterno, unite alla necessità di sfruttare tutte le potenzialità della tecnologia e dei servizi innovativi sul cliente, comportano il fatto che anche le strategie di protezione degli asset aziendali vengano costantemente monitorate e adattate alle più ampie strategie aziendali*
*(es. soglie di rischio dinamiche nel medio periodo, ridistribuzione degli investimenti, accettazione tattica del rischio, ..)*

# L'evoluzione degli attacchi alle banche

L'attività tipica della banca, unita al suo ruolo di primo piano nel sistema economico e finanziario territoriale, la rende soggetta a minacce - quali il cybercrime - che sfruttano le **VULNERABILITÀ** connesse alla tecnologia e alle persone per **FINALITÀ** sia economiche ("Guadagno") che dimostrative o destabilizzanti ("Geopolitica") .
Questo contesto, facilitato dalla disponibilità sempre maggiore di tecnologia a basso costo, crea **scenari di rischio in continua evoluzione con impatti spesso trasversali** su tutte le aree della sicurezza.

*È necessario che la struttura di Governance della Sicurezza riveda le proprie priorità di protezione sia in funzione dell'evoluzione del business sia in funzione delle dinamiche con cui evolvono gli attacchi*




**Tecnologia** (Malware, DDoS, Cross Channels, Apps)
**Persona** (Social Engineering, Cliente, personale interno / outsourcer)

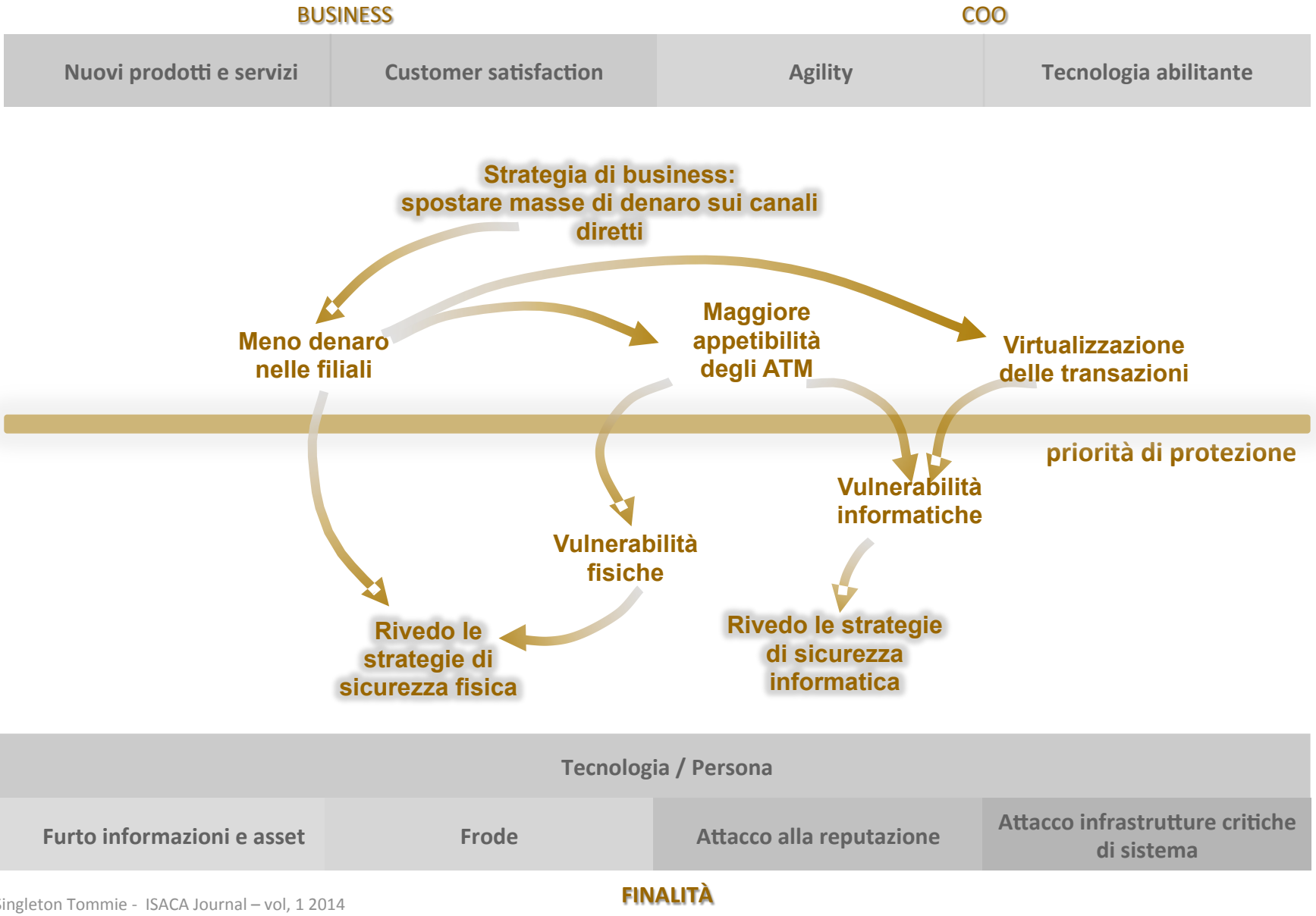
**VULNERABILITÀ**

| Furto informazioni e asset | Frode | Attacco alla reputazione | Attacco alle infrastrutture critiche di sistema |
|---|---|---|---|

Guadagno — **FINALITÀ**[1] — Geopolitica

[1] Singleton Tommie - ISACA Journal – vol, 1 2014

# Un esempio di Governance trasversale alle aree di sicurezza fisica e informatica

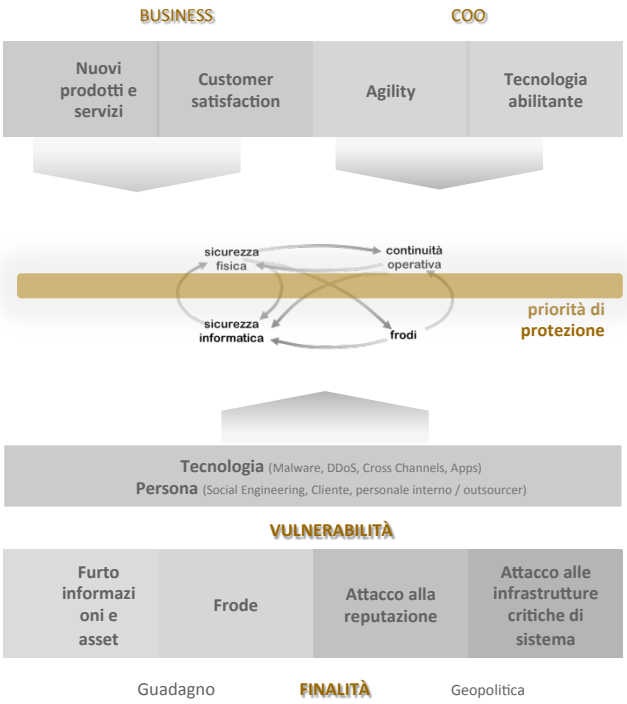



(1) Singleton Tommie - ISACA Journal – vol, 1 2014

# Il nuovo contesto bancario richiede l'attivazione di nuovi equilibri di sicurezza

L'evoluzione del contesto di business e operativo della banca e la trasformazione continua delle minacce cui questa è sottoposta, richiede alle Funzioni di Governance della Sicurezza di definire le proprie priorità di protezione ponendosi precisi obiettivi di equilibrio nella scelta:

- dell'adeguato **mix di contromisure**
- della **coerenza delle strategie operative**




equilibrio

## Contromisure

- di processo / tecnologiche
- mature / innovative
- personalizzate / di mercato

## Strategie

- utilizzo risorse interne ed esterne
- mitigazione del rischio e efficienza degli investimenti
- breve e medio periodo
- consapevolezza del vertice e responsabilità di accettazione del rischio

obiettivi

## Fiducia e Credibilità

- Affidabilità
- Reputazione
- Comunicazione
- …

## Tecnologia Sicura

- Cloud
- Big data
- NFC
- Mobile
- …

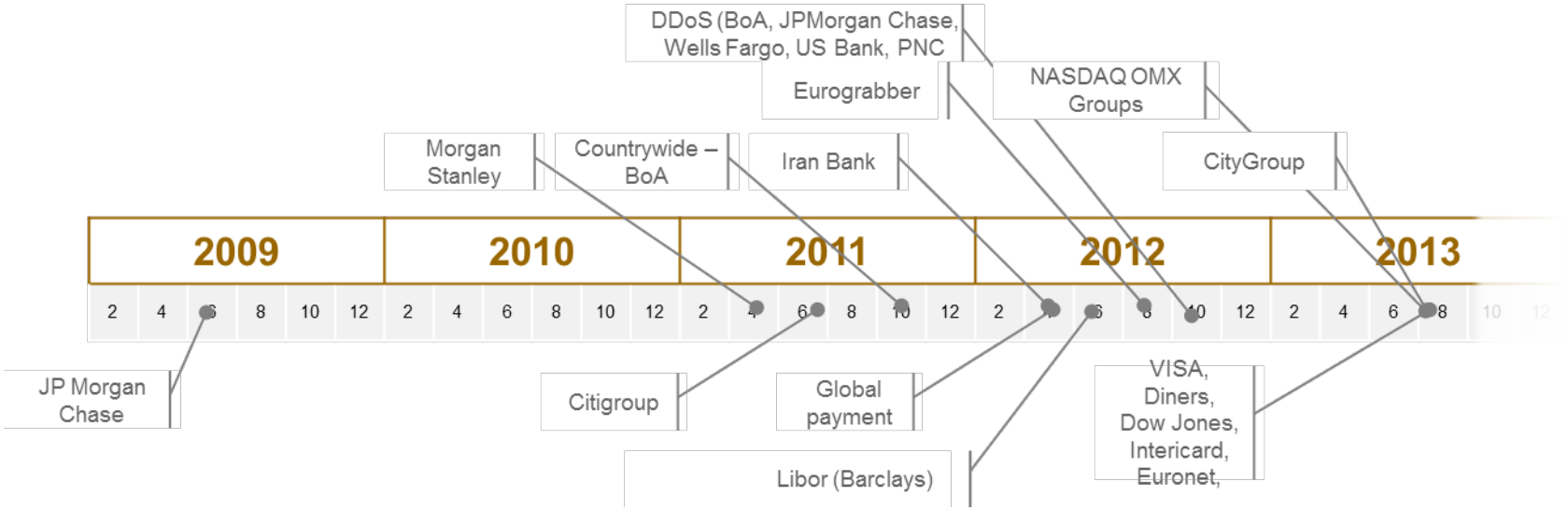
## Sviluppo nuovi prodotti e servizi

- Carte
- Dematerializzazione
- Nuovi sistemi di pagamento
- …

- Il contesto legislativo
- Il contesto di business e operativo
- **L'evoluzione degli scenari**
- L'approccio basato sul rischio
- Alcuni spunti di riflessione

# L'evoluzione degli incidenti di sicurezza in ambito Finance degli ultimi anni

Una breve analisi dello storico degli incidenti di sicurezza degli ultimi anni nel settore finance conferma il **trend in costante aumento degli incidenti**, soprattutto per quelli derivanti da attacco esterno strutturato e mirato.
La rappresentazione grafica dello storico relativo agli incidenti IT conferma la necessità di garantire al mercato una sempre **maggior attenzione a questa tipologia di eventi** anche a livello **istituzionale e governativo** (cfr. Obama Act)



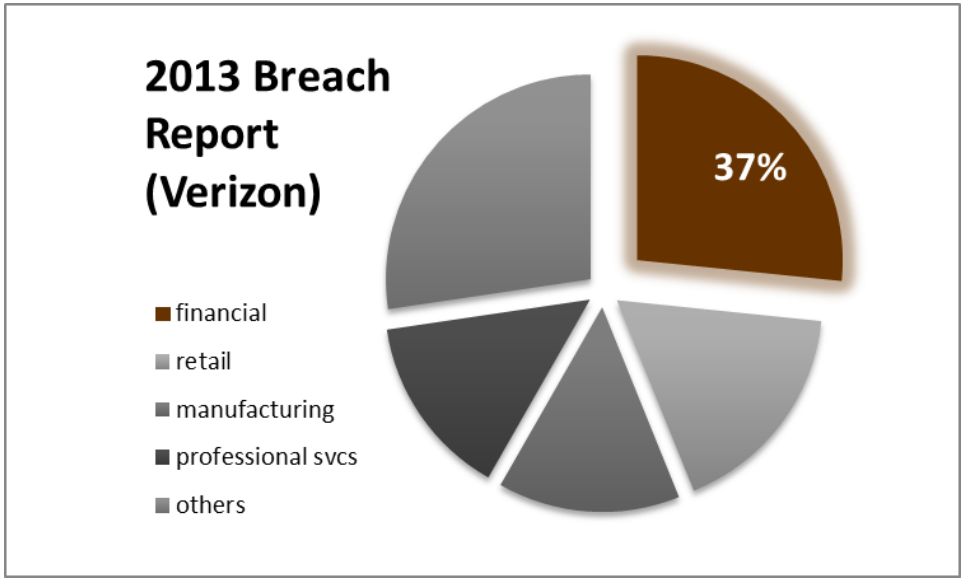

Seppur solo rappresentativa del trend di incremento degli incidenti di sicurezza, la sintesi dei principali eventi degli ultimi 4 anni permette di evidenziare come le cause di accadimento degli incidenti stessi possano essere ricondotte a specifiche tipologie di minacce:

- errore interno
- dolo da parte di dipendenti
- contromisure deboli o assenti
- attacco strutturato dall'esterno

Source: DataBreaches.net, IdTheftCentre, press reports - Research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson - money.cnn.com/2012/09/27/technology/bank-cyberattacks/) - www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

# L'evoluzione degli scenari di sicurezza in ambito Finance prevista per i prossimi anni

Il settore finance è - e molto probabilmente continuerà ad esserlo - uno dei principali settori su cui si concentreranno gli attacchi che avranno livelli di complessità sempre crescente e che richiederanno risposte sempre più integrate e trasversali alle Funzioni della banca




| minacce esterne | incidenti | complessità | governance |
|---|---|---|---|
| Il 59% delle aziende nel settore finance prevede nel breve un aumento delle minacce esterne | Per il 44% delle aziende finanziarie il numero degli incidenti di sicurezza è significativamente aumentato (dal 5 al 25%) rispetto l'anno precedente | Il 38% delle aziende nel settore finance ritiene che gli attacchi esterni sono sempre più sofisticati e articolati (es. cross-channel) | Il 61% delle aziende nel settore finance ritiene che l'adozione ed il mantenimento di standard internazionali e relative certificazioni hanno massima o alta priorità per i CSO |

Livello di incremento atteso: Min Max

*Source:*
*EY – Oct. 2013 - Under cyber attack - EY's Global Information - Security Survey 2013*
*PwC - Sept. 2013 – "Key findings from The Global State of Information Security® Survey 2014"*

# I nuovi scenari di sicurezza determinano nuovi obiettivi per la Governance di Sicurezza

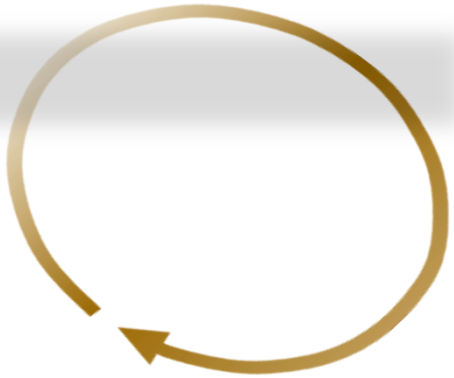
L'analisi delle tendenze passate e future richiede alle Funzioni di Governance della Sicurezza delle banche di focalizzarsi, per rispondere in maniera adeguata all'evoluzione degli scenari di rischio, su specifici obiettivi di **prevenzione**, **monitoraggio e sintesi** e di **velocità di risposta**

## Monitoraggio e sintesi

- Gestione delle soglie di allerta
- Aggiornamento frequente dei dati e delle informazioni

## Prevenzione

- Analisi evoluzione minacce
- Controlli sull'efficacia delle soluzioni di sicurezza
- Test di sicurezza nel ciclo di vita dei prodotti e degli asset aziendali



## Velocità di risposta

- CSIRT (Computer Security Incident Response Team)
- Condivisione obiettivi e processi di sicurezza
- Modelli integrati di gestione degli incidenti e delle situazioni di crisi

- Il contesto legislativo
- Il contesto di business e operativo
- L'evoluzione degli scenari
- **L'approccio basato sul rischio**
- Alcuni spunti di riflessione

# L'approccio basato sul rischio come fattore abilitante per una sicurezza a valore aggiunto

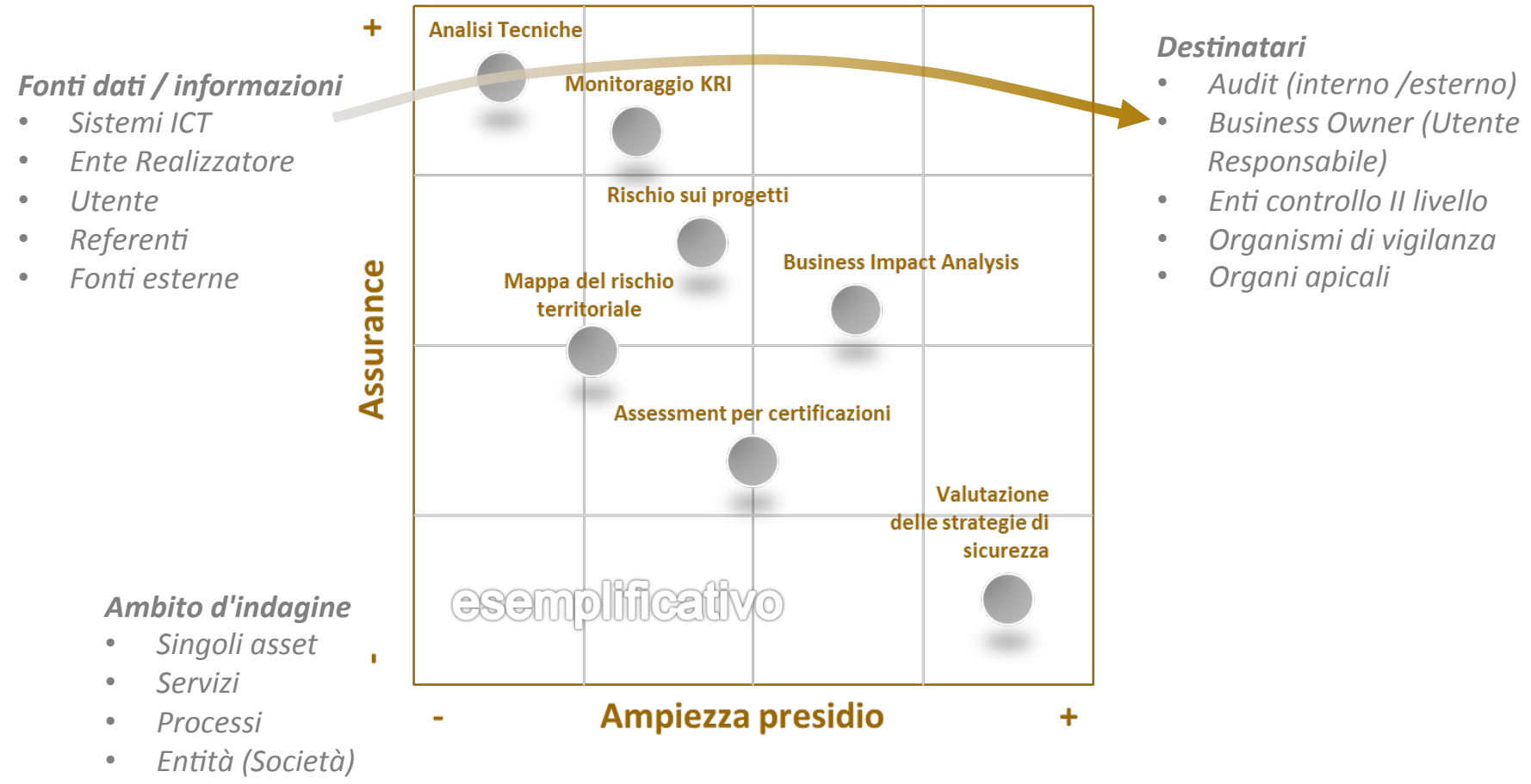
I contesti legislativi e operativi nei quali la banca persegue il proprio business, uniti all'evoluzione degli scenari di rischio, pongono delle specifiche esigenze alle Funzioni di Governance della Sicurezza che possono essere affrontate mediante un approccio basato sull'**analisi e il governo del rischio**.

Il governo strutturato e continuo dei livelli di rischio permette di individuare parametri e soglie di accettabilità del rischio che tengano in considerazione le specificità delle diverse aree di sicurezza e dei loro **punti di integrazione**, che spesso si rivelano il **punto debole** su cui si concentrano gli attacchi esterni. La comprensione del livello di rischio complessivo permette di prendere in considerazione gli aspetti eterogenei della sicurezza e di individuare e sviluppare contromisure efficaci e adeguate alle richieste del contesto interno e esterno

| Contesto legislativo | Contesto di business e operativo | Evoluzione degli scenari |
|---|---|---|
| **Nuovi strumenti** per rispondere ai requisiti normativi italiani e europei | **Nuovi equilibri** nei mix di contromisure e nel mix di strategie | **Nuovi obiettivi** per prevenire gli attacchi e rispondere in tempo reale |

# Gli strumenti e le potenzialità dell'approccio basato sul rischio

L'approccio basato sul rischio deve disporre di una serie di **strumenti** che nel loro insieme garantiscano la copertura delle diverse esigenze di Governo della Sicurezza.
I risultati dei singoli strumenti di governo del rischio devono essere integrati e aggregati in funzione delle specifiche **esigenze degli interlocutori** garantendo una **sintesi efficace**, con contenuti che non richiedano necessariamente ai destinatari delle competenze specialistiche.



- Il contesto legislativo
- Il contesto di business e operativo
- L'evoluzione degli scenari
- L'approccio basato sul rischio
- **Alcuni spunti di riflessione**

- Il **contesto in cui opera la banca è in continua e rapida evoluzione**, sia dal punto di vista economico e culturale (es. aspettative del mercato, capacità di utilizzo delle tecnologie, ...) sia dal punto di vista normativo e giuridico (es. circolare 263 Banca d'Italia, nuovo ruolo della BCE, …).

- La banca pone sempre più **attenzione alla qualità e al tasso di innovazione** delle proprie attività (es. qualità degli investimenti, rilascio di servizi "di frontiera" alla clientela, gestione integrata dei rischi,…).

- La sicurezza assume un ruolo sempre più vicino al business, evolvendo dal tradizionale compito di messa in sicurezza dei processi operativi aziendali verso una mansione focalizzata ad **abilitare nuovi servizi e prodotti a valore per la clientela.**

- Gli **incidenti accadono**. Non sono solo numeri statistici "lontani" ma vere e proprie fonti di preoccupazione dei vertici decisionali, a livello nazionale e non solo (es. Obama Act, individuazione dei CSIRT a livello europeo, ..)

- Gli **attacchi sono sempre più sofisticati e trasversali** e utilizzano tecnologie a costo sempre più basso (es. inefficacia delle contromisure "standard di mercato" rispetto a soluzioni di copertura delle vulnerabilità peculiari della banca,..) determinando la necessità di sempre **maggior integrazione e complementarietà** tra le varie aree di sicurezza nella ricerca di soluzioni che combinino al loro interno tutte le dovute contromisure.

- Il **Governo del Rischio**, integrandosi nel sistema dei controlli complessivi della banca e dovendo analizzare tutte le componenti a prescindere dall'area di sicurezza di pertinenza, **è un approccio che riesce a sostenere le richieste interne ed esterne** in termini di:
  - consapevolezza dei vertici aziendali sullo stato di sicurezza aziendale
  - individuazione degli obiettivi e delle priorità di protezione
  - ottimizzazione degli investimenti
  - incremento dell'efficienza (produttività / innovazione)
  - soddisfazione stakeholders (clienti, collaboratori, regolamentatori)

INTESA SANPAOLO
GROUP SERVICES

***La consapevolezza del rischio come base per il Governo della Sicurezza di Gruppo***

# Grazie per l'attenzione

Alberto Sferch
Responsabile Governo Sicurezza e Continuità Operativa