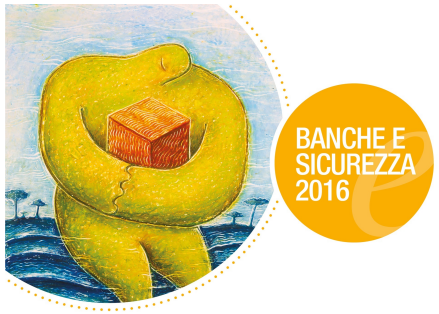
BANCA POPOLARE DI MILANO



Il futuro è di chi fa.

Sicurezza, Rischio e Business Continuity
Quali sinergie ?

ABI Banche e Sicurezza 2016

John Ramaioli

Milano, 27 maggio 2016

Agenda

- Il contesto normativo ed organizzativo
- Possibili sinergie
- Considerazioni finali

Il contesto normativo

Le normative esterne, disposizioni di settore e standard di riferimento anche di recente emanazione definiscono **un approccio che in genere contempla** definizione di una metodologia, formalizzazione ruoli e responsabilità e esecuzione dei controlli; si individuano inoltre una **serie di elementi comuni**

- Disposizioni di Vigilanza Prudenziale (285/13)
- Sicurezza pagamenti su internet (BCE, EBA, PSD)
- Tutela del risparmio e mkt finanziari (262/2005)
- Responsabilità amministrativa (231/2001)
- Tutela della privacy (GDPR e 196/93)
- Framework Nazionale per la Cybersecurity
- ……..

- Coinvolgimento figure apicali
- Misure di sicurezza e continuità congrue con il rischio
- Approccio risk based
- Sistema integrato controlli
- Analisi su Processi e Asset
- Tracciatura degli incidenti
- Reportistica e trasparenza
- Awareness utenti e clienti

Il contesto organizzativo

Diverse strutture aziendali esercitano i controlli di competenza con un approccio a «Silos»

Funzioni di Controllo

Compliance	Risk Management	Audit	.....	Regulators / revisori
Conformità alla Normativa vigente	Determinazione livelli di rischio operativo / informatico	Verifica agito nei processi di erogazione		Analisi dei modelli di governo dei rischi e della sicurezza

Funzione Sicurezza

- Riceve **richieste simili** da molti interlocutori differenti
- **Analizza le normative** di pertinenza o con impatto sulla sicurezza
- Svolge **attività di controllo** di propria responsabilità
- Assume **funzione di «consulente» e facilitatore** fra diverse interlocutori

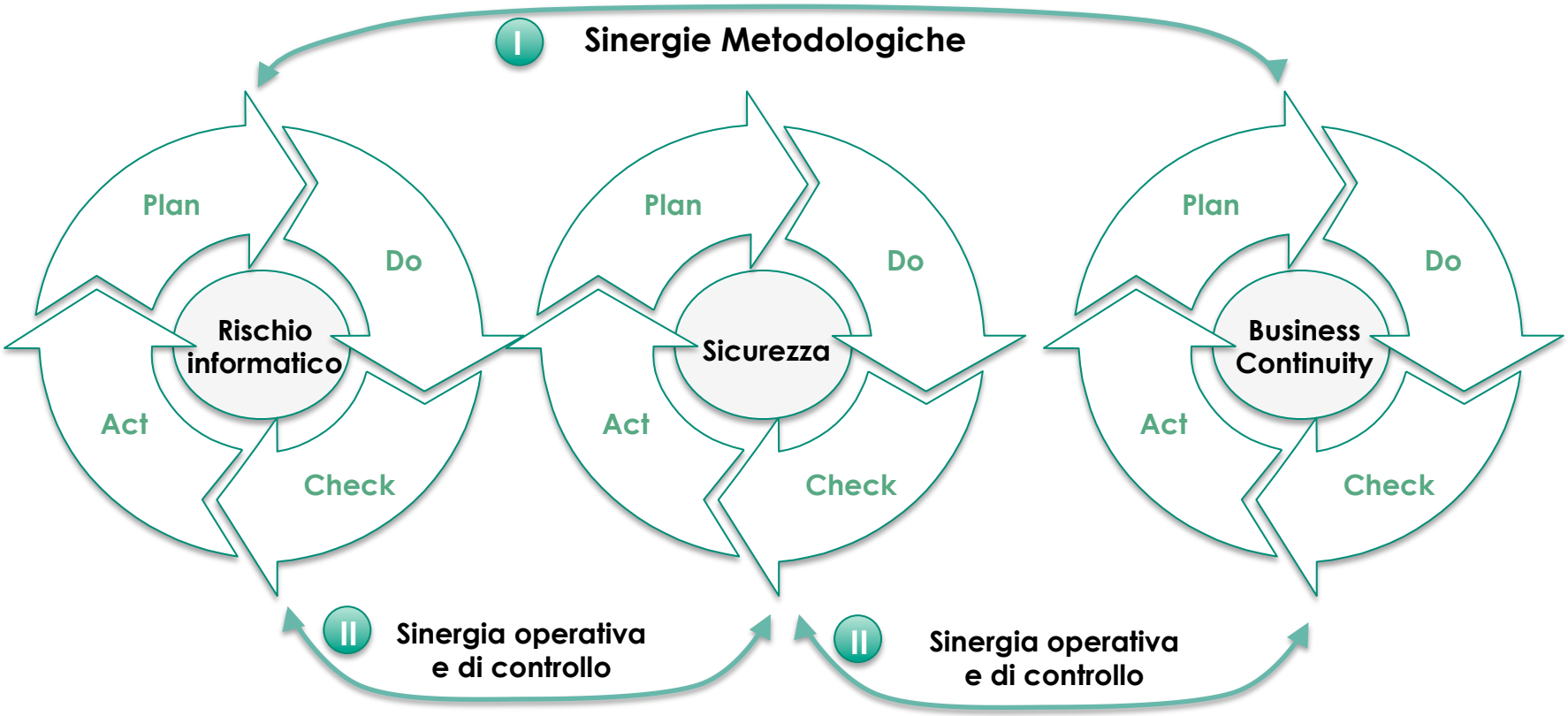
Emerge una forte **esigenza di razionalizzare** le proprie attività e di ridurre l'effort a limitato valore aggiunto

Agenda

- Il contesto normativo ed organizzativo
- Possibili sinergie
- Considerazioni finali

La ricerca delle Sinergie

Diverse discipline evolvono secondo metodologie proprie ma hanno importanti punti di contatto



Policy

Awareness

Sinergie fra Rischio informatico e Business Continuity

Rischio informatico e Continuità Operativa possono essere gestiti in modo estremamente vantaggioso per la Banca, adottando una **metodologia integrata** a fronte dei numerosi aspetti comuni in termini di **approccio**, **processo** e **responsabilità**

I

Tassonomia dei processi aziendali - approccio process oriented
La valutazione degli impatti sui processi aziendali viene effettuata partendo dalla tassonomia dei processi della Banca

II

Enterprise Architecture
Disponibilità ed affinamento *della mappatura dei componenti informatici / infrastrutture di base afferenti i processi di business come base per valutare l'esposizione al rischio informatico e l'indisponibilità dei servizi IT*

III

Owner di processo e referenti IT.
Coinvolgimento dei medesimi process owner per la raccolta delle valutazioni di impatto e delle stesse strutture specialistiche IT per la valutazione delle componenti informatiche

IV

Raccordo con funzioni di controllo
Raccordo con la politica complessiva di gestione del rischio della banca e con il relativo livello di accettazione del rischio (RAF); contributo similare al Sistema Integrato dei Controlli

V

Coinvolgimenti vertici aziendali
I vertici aziendali *(OFSS, OFG e l'Organo con Funzione di Controllo) sono coinvolti, per entrambe le discipline, nel ruolo di indirizzo e ricevono reportistiche omogenee in ottica di approvazione e controllo*

Sinergie fra Rischio Informatico, Sicurezza e Business Continuity

Attività operative, quali la ***gestione degli incidenti di sicurezza*** e ***la gestione delle frodi informatiche***, se condotte con una visione sinergica, possono *alimentare* ***la continua evoluzione*** dei singoli processi di gestione del rischio informatico e della sicurezza

I

Oggettivazione delle analisi
L'introduzione di informazioni reali ed oggettive trasversali a differenti tipologie di eventi aumenta la capacità di rendere più robusta e meno soggettiva la fase di valutazione dei rischi

II

Efficacia delle misure di sicurezza
La condivisione delle attività di gestione degli eventi permette di creare sinergie importanti in termini di idoneità e gradualità delle contromisure tecnologiche e/o organizzative e di tempestività di intervento

III

Reportistica integrata
La creazione di report integrati verso i vertici aziendali viene facilitata dalla capacità di sviluppare indicatori omogenei e di definire e alimentare un unico archivio di informazioni rilevanti

IV

Processo di escalation ed Integrazione tra Incident e crisis management
La gestione dei vari incidenti di sicurezza abbinata alla pluriennale esperienza sulla BC permette di utilizzare gli stessi meccanismi di escalation ed attivare le stesse strutture preposte alla crisi in particolare per lo scenario Cyber

Sinergie fra differenti esigenze di controllo

Gran parte dei controlli di sicurezza fanno spesso riferimento ad alcuni standard riconosciuti internazionalmente: sono quindi **trasversali** e possono essere **messi a fattor comune,** rispondendo alle esigenze di verifica della sicurezza, alle necessità di compliance e a quelle delle Funzioni di Controllo aziendali.

I **Ottimizzazione a armonizzazione**
Individuazione e descrizione dei controlli e relativa frequenza in relazione al rischio e/o ai differenti sottosistemi tecnologici

II **Mappatura dei controlli con principali normative**
Analisi e individuazione controlli richiesti dalle normative (231, AdS, Privacy) e efficaci anche in risposta alle richieste delle FdC / revisori

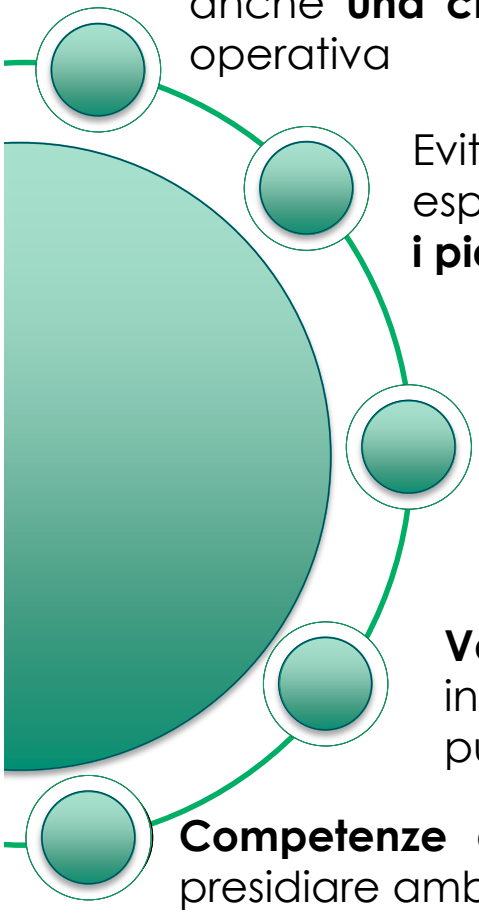
III **Raccolta evidenze**
Creazione repository centralizzato per raccolta evidenze dei controlli eseguiti e delle eventuali anomalie riscontrate

IV **Reporting a funzioni apicali**
Relazione periodica dello stato dell'arte della «sicurezza» con individuazione delle operazioni anomale riscontrate per Organi e funzioni di Controllo

Agenda

- Il contesto normativo ed organizzativo
- Possibili sinergie
- Considerazioni finali

Considerazioni finali…



Sinergie tra discipline «confinanti» rappresentano non solo una necessità, ma anche **una chiara opportunità** per ottenere benefici in termini di efficienza operativa

Evitare approccio *a silos* consente di mettere a fattor comune le esperienze e, di conseguenza, a meglio **indirizzare la strategia ed i piani evolutivi della Sicurezza**

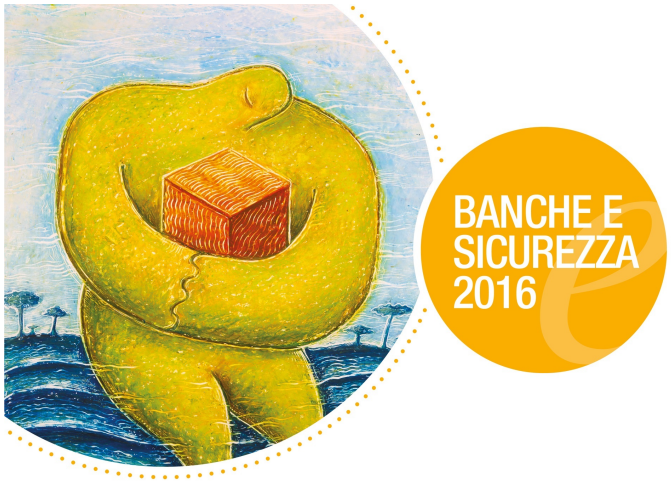
Fattore abilitante è certamente la possibilità di identificare un'unica ***funzione specialistica*** che rappresenti su tutti questi temi il focal point per organi apicali, funzioni di Business e di controllo

Valorizzazione delle persone che sanno «leggere» in modo integrato le diverse normative e suggerire approcci sinergici pur nella peculiarità delle singole discipline

Competenze diversificate ed interfunzionali sempre più necessarie per presidiare ambiti e discipline solo all'apparenza differenti e separate

BANCA POPOLARE DI MILANO

Il futuro è di chi fa.



Grazie per l'attenzione!

John Ramaioli

Banca Popolare di Milano
Sicurezza e Business Continuity

john.ramaioli@bpm.it