INTESA SANPAOLO

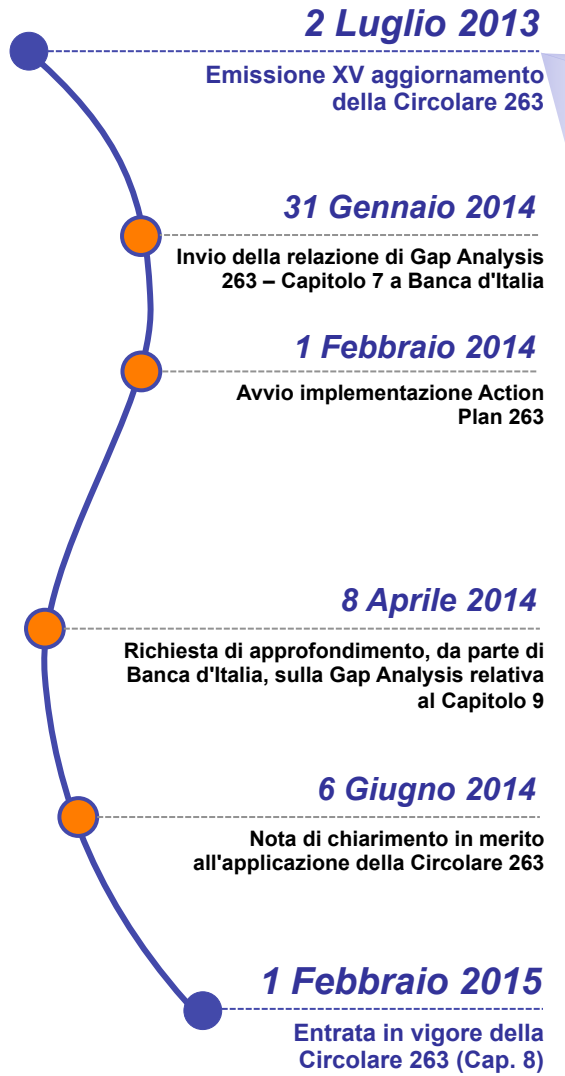
Banche e Sicurezza 2015

Sicurezza informatica: Compliance normativa e presidio del rischio post circolare 263

Leonardo Maria Rosa
Responsabile Ufficio Sicurezza Informatica

5 giugno 2015

Premessa
Il percorso di adeguamento alla Circolare 263



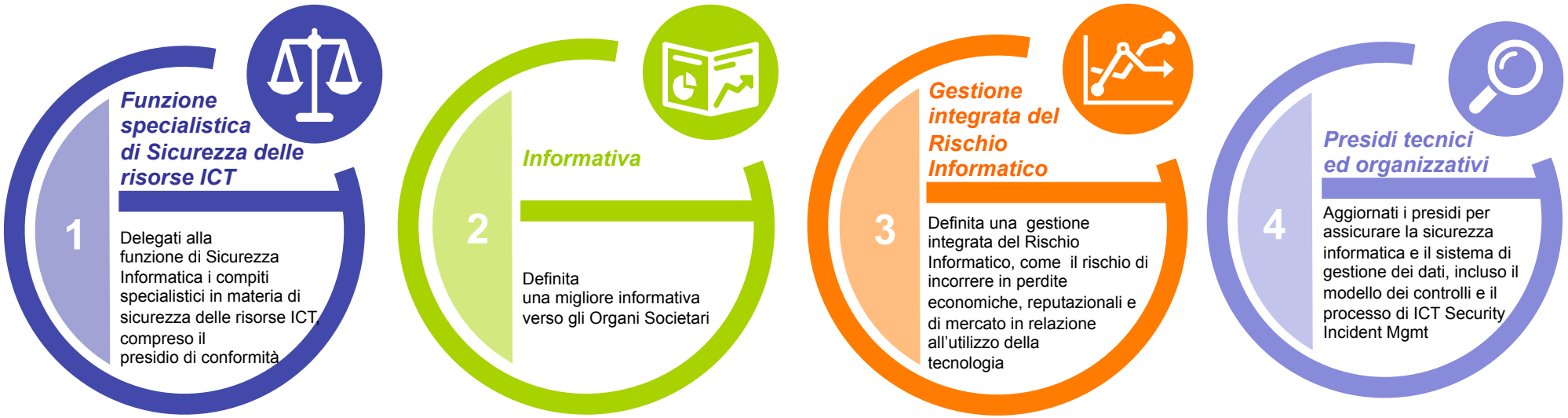
Le "**Nuove disposizioni di vigilanza prudenziale per le banche**" introducono, come elemento di novità:

- il Capitolo 7 "**Il sistema dei controlli interni**";
- il Capitolo 8 "**Il sistema informativo**";
- il Capitolo 9 "**La continuità operativa**";

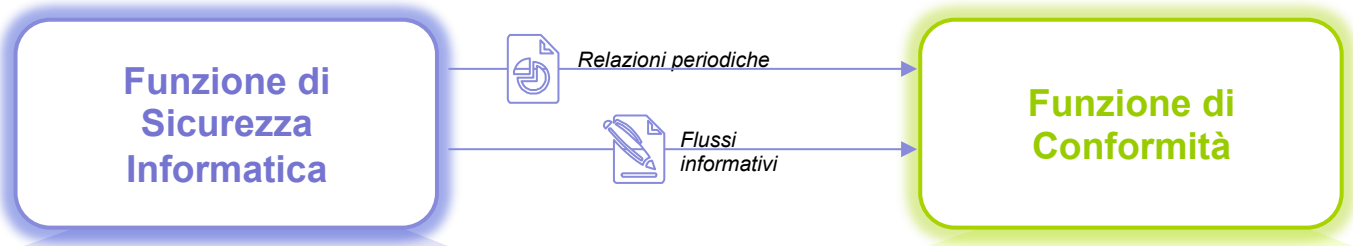
richiedendo ai destinatari della normativa di condurre un'autovalutazione della propria situazione rispetto alle previsioni della norma ("**Gap Analysis**") e di avviare le opportune azioni di adeguamento ("**Action Plan 263**").

Premessa
Principali interventi in materia di Sicurezza Informatica

Il Gruppo Intesa Sanpaolo ha **avviato** un **insieme di attività** finalizzate ad adeguare la **gestione** della **sicurezza informatica** del Gruppo introducendo **nuove modalità operative**.



I principali interventi definiti nel contesto di Intesa Sanpaolo
Presidio di conformità della normativa in materia di sicurezza informatica



La **Funzione di Sicurezza Informatica** riveste il ruolo di **Funzione Specialistica di Gruppo in materia di sicurezza informatica:**

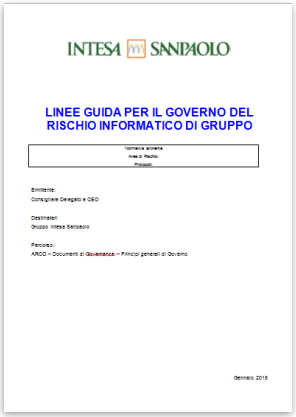
- **Funzione specialistica di conformità** rispetto ai temi di sicurezza informatica, incluso il presidio dei controlli;
- A**ggiornamento** ed **integrazione dell'impianto normativo interno** al fine di garantire la rispondenza con la normativa esterna, i principali standard internazionali e best practices di settore.

La **Funzione di conformità** esprime, sulla base delle informazioni fornite dalla Funzione di Sicurezza Informatica e dalle verifiche direttamente condotte, una **valutazione autonoma** in merito a:

- **rischio di non conformità** alla normativa in materia di Sicurezza Informatica;
- **adeguatezza dei presidi posti in essere** per la relativa mitigazione e, ove ne ravvisi la necessità, richiede di dare corso agli opportuni interventi di rafforzamento.

I principali interventi definiti nel contesto di Intesa Sanpaolo
Gestione integrata del rischio informatico

Intesa Sanpaolo ha definito un processo di **analisi** e **valutazione del Rischio Informatico di Gruppo** coordinato dalla funzione Risk Management a cui concorrono le **funzioni aziendali** competenti, il **business** e **le funzioni di controllo:**


INTESA SANPAOLO

LINEE GUIDA PER IL GOVERNO DEL RISCHIO INFORMATICO DI GRUPPO

Gennaio 2015

Le **Linee Guida per il governo del rischio informatico di Gruppo** definiscono :

- **Fasi del processo** di governo del Rischio Informatico;
- **Ruoli e responsabilità** degli Organi Societari e delle Funzioni aziendali coinvolte;
- Flussi di aggiornamento verso gli Organi Aziendali.

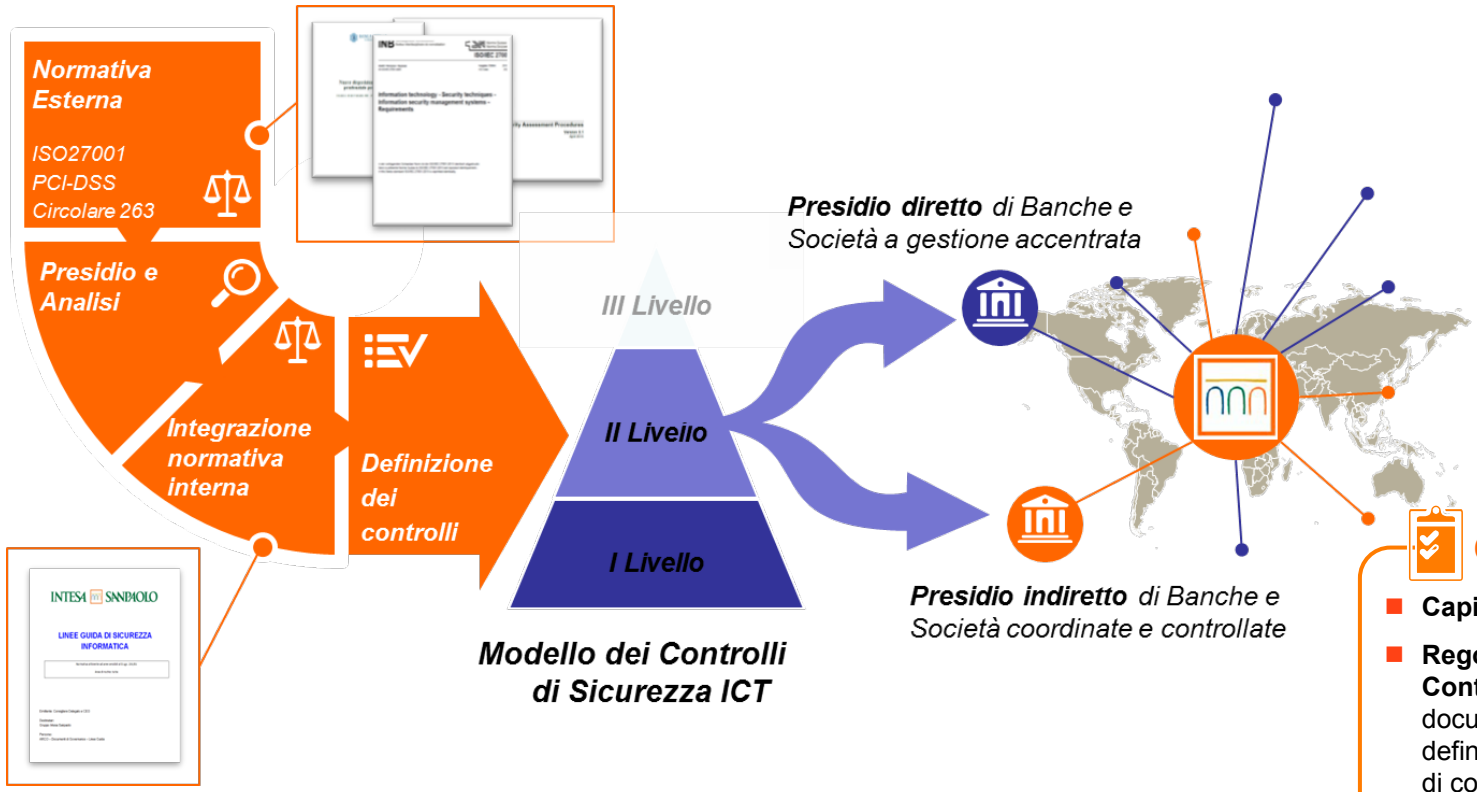
La nuova metodologia di analisi del rischio ICT viene applicata:

- **annualmente**, per eseguire una **valutazione complessiva del Rischi ICT o delle procedure in esercizio**;
- **ad evento**, in presenza **di situazioni che possono modificare il complessivo livello di rischio** (ad es. gravi incidenti, diffusione di notizie su nuove vulnerabilità o minacce) ovvero in caso di progetti innovativi o modifiche a componenti.

*La Funzione di Sicurezza Informatica **conduce** in modo autonomo un'analisi periodica del Rischio di Sicurezza Informatica **e contribuisce**, con questa, **al processo integrato** del più generale Rischio Informatico.*

I principali interventi definiti nel contesto di Intesa Sanpaolo
Modello dei controlli di sicurezza informatica (1 di 2)

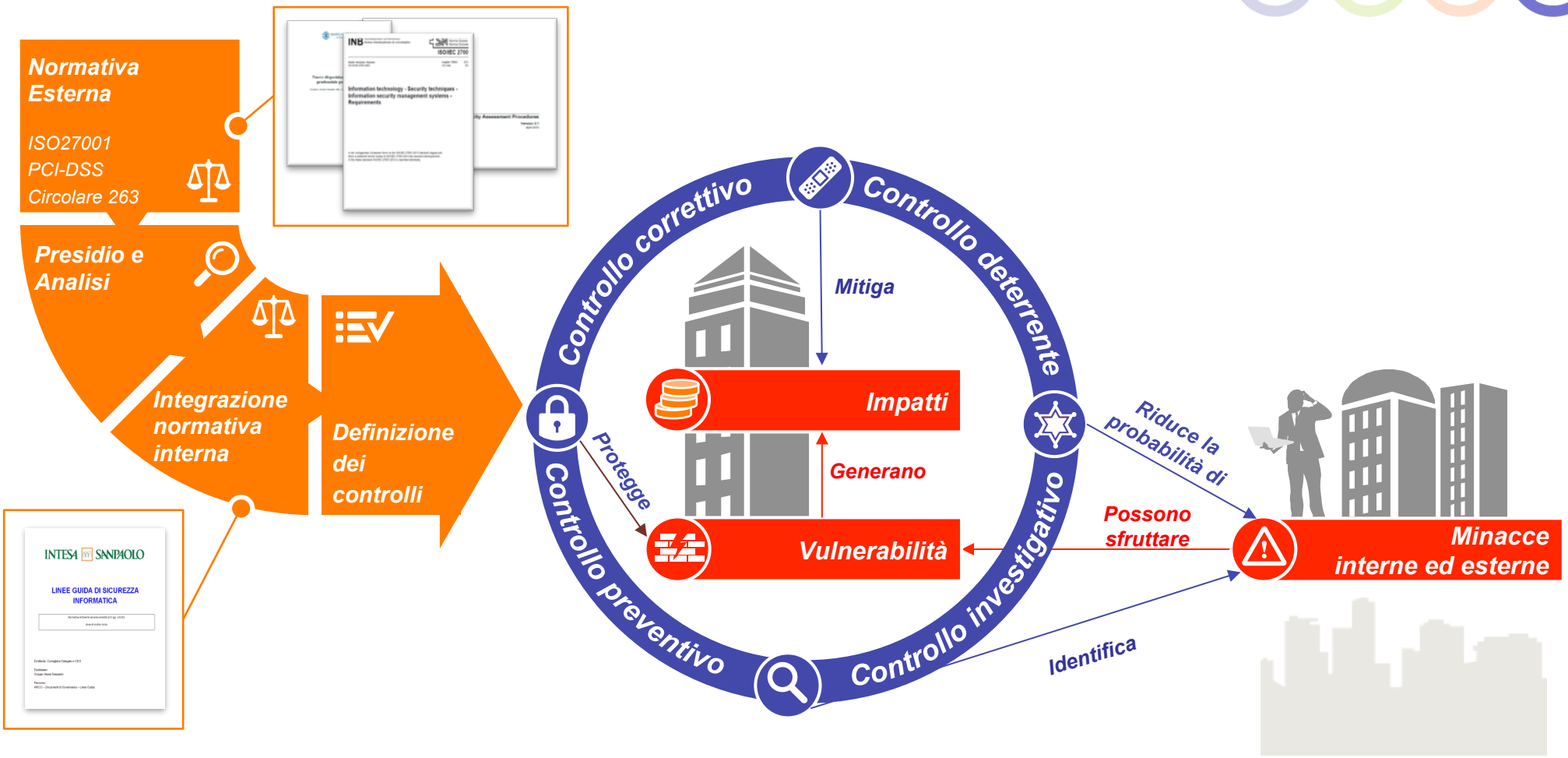
Il Gruppo Intesa Sanpaolo ha **aggiornato** e **formalizzato** il modello di **gestione dei controlli interni** in ambito Sicurezza Informatica:



Compliance

- **Capitolo 7** - **Circolare 263**;
- **Regolamento del Sistema dei Controlli Interni Integrato**, documento di governance che definisce le responsabilità, modalità di coordinamento e i flussi informativi degli Organi e delle funzioni con compiti di controllo.

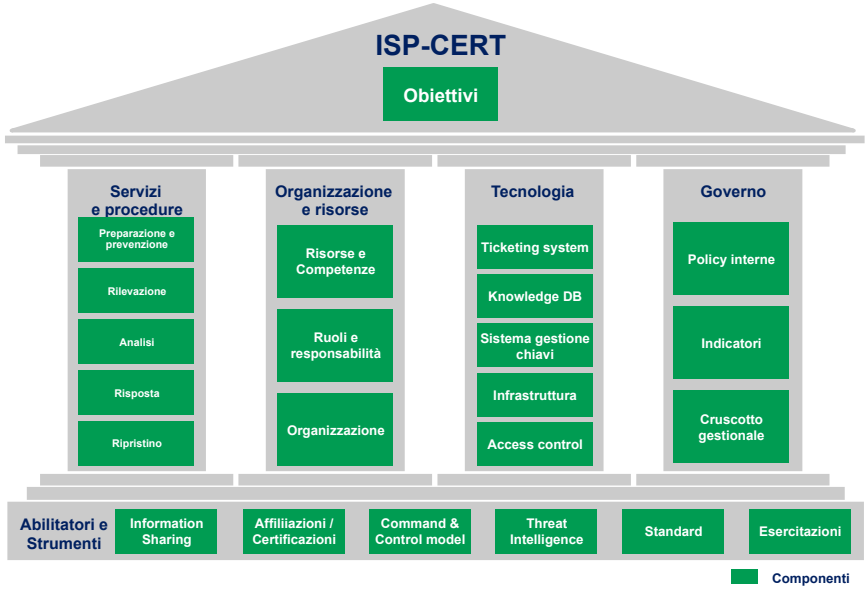
I principali interventi definiti nel contesto di Intesa Sanpaolo
Modello dei controlli di sicurezza informatica (2 di 2)



I principali interventi definiti nel contesto di Intesa Sanpaolo
Integrazione tra i processi di Incident e Crisis Management

Intesa Sanpaolo ha **avviato** una serie di **attività di adeguamento** atte a **rafforzare** il processo di **ICT Security Incident Management:**

Componenti del modello operativo ISP-CERT



- Istituzione di un **Computer Emergency Response Team** (**CERT**) interno;
- **Presidio** costante, mediante un'attività di **intelligence**, dell'evoluzione degli **scenari di attacco** allo scopo di **individuare** ed **anticipare** le possibili **minacce**;
- **Raccordo** del **CERT con gli altri presidi interni** ad Intesa per la gestione degli incidenti (es. Incident Management, MOGC, SOC, etc.);
- **Indirizzo** dell'attività di **estensione** delle modalità operative individuate **a tutte le Società del Gruppo** Intesa Sanpaolo.

Le modalità di attuazione sulla Banche e Società del Gruppo
Modalità di gestione e piano di roll-out

Intesa Sanpaolo ha avviato un **programma strutturato** per assicurare il recepimento e il rispetto degli **indirizzi di Information Security** definiti da Capogruppo **da parte delle Banche** e **delle Filiali estere**, garantendo così la **coerenza** con gli **obiettivi strategici** sulle tematiche di Information Security definiti a livello di Gruppo

Razionali

- **assetti organizzativi** accentrati o meno rispetto a Capogruppo
- **vincoli normativi** o **esigenze di business** legate allo specifico contesto
- **modalità operative consolidate** nel tempo

Modello di Gestione

Società con Gestione accentrata

Legal Entity per le quali **Capogruppo**, interagendo con un eventuale Referente di Sicurezza, **indirizza in modo centralizzato le tematiche** legate alla **Sicurezza Informatica**, secondo principi e modelli di Governance definiti a livello di Gruppo.

Società coordinate e controllate

Legal Entity italiane ed estere che **indirizzano in modo autonomo**, sotto il controllo del proprio Responsabile di Sicurezza, **le tematiche** legate alla **Sicurezza Informatica**, ma sempre tramite il coordinamento e il controllo di Capogruppo che detta i principi di Governance validi a livello di Gruppo

Perimetro di applicazione

- **74** *Banche e Società Italiane*
- **15** *Uffici di Rappresentanza*
- **13** *Filiali Corporate*
- **12** *Banche Estere*
- **3** *Banche Corporate*

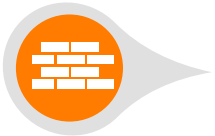
Conclusioni

Il **XV aggiornamento della Circolare 263** ha rappresentato **per tutto il settore bancario** un'importante **opportunità di crescita**, specie per quel che riguarda il presidio delle tematiche legate alla sicurezza informatica.

identificare in modo tempestivo **i possibili rischi ai quali l'organizzazione può essere esposta**, in modo da **intraprendere le necessarie contromisure** affinché questi risultino accettabili;

definire un approccio risk-based per la gestione dei sistemi informativi indirizzando, in modo opportuno, investimenti e strategie;

monitorare costantemente **l'efficacia delle misure di sicurezza implementate**, avendo una **visione** consapevole **degli scenari di minaccia** non solo interni, ma anche esterni;



costruire un'efficace e concreta difesa partendo dalle informazioni riguardanti gli attacchi subiti;

comunicare direttamente con il business ed **ottenere** ulteriore **commitment sulle tematiche** legate all'**Information Technology**.