

**INTESA  SANPAOLO**

**FCC Forum**

**Metodologie e processi di gestione del rischio e di  
contrasto dell'illecito: il ruolo della funzione di  
conformità alle norme**

Intervento di Piero Boccassino

Group Chief Compliance Officer di Intesa Sanpaolo

4 Dicembre 2020

# INDICE



## **Il rischio di non conformità nel sistema integrato di gestione dei rischi**



Il modello adottato da Intesa Sanpaolo



Il contrasto agli illeciti e la collaborazione attiva con le Autorità



Le sfide future



Allegati

# Il rischio di non conformità alle norme ...

- Il **rischio di non conformità (cd non-compliance risk)** è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazione di norme imperative (leggi, regolamenti) ovvero di autoregolamentazione (ad es. statuti, codici di condotta, codici di autodisciplina).
- Il rischio di non conformità è riconducibile, per la parte relativa alle sanzioni ed alle perdite finanziarie, al **rischio operativo** e, per i danni di reputazione, al **rischio reputazionale**.
- Il rischio di non conformità ha importanti aree in comune con il **rischio di condotta (cd conduct risk)** definito come il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di comportamenti:
  - non corretti nei confronti della clientela (misselling);
  - che mettano a rischio l'integrità e il regolare funzionamento dei mercati (market integrity);
  - che costituiscano violazione della normativa in ambito financial crime (antiriciclaggio, antiterrorismo, embarghi, anticorruzione, cyber crime).



## Principale normativa di riferimento

-  Guidelines on Corporate Governance principles for banks, Basel Committee, 2015
-  Guidelines on Internal Governance, EBA, 2017
-  Guidelines on certain aspects of the MiFID compliance function requirements, ESMA, 2019
-  Direttiva 2009/138/CE Solvency II
-  Circolare 285, Parte Prima, Titolo IV, Banca d'Italia
-  Regolamento Banca d'Italia 5 dicembre 2019
-  Regolamento Intermediari Consob
-  Regolamento 28/2018 IVASS
-  Guidelines on common procedures and methodologies for the SREP, EBA, 2014
-  Report on misconduct risk in the banking sector, ESRB, 2015

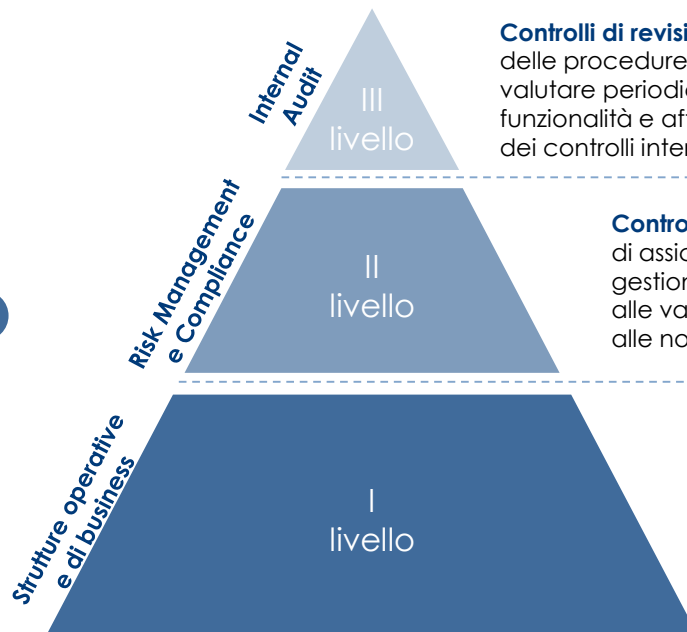
# ...nel sistema integrato di gestione dei rischi

La **gestione del rischio di non conformità** si colloca nell'ambito del **sistema integrato di controlli interni** a presidio dei rischi dell'intermediario, che vede una struttura caratterizzata da **tre livelli di presidio** svolti da **distinte funzioni aziendali**

## Marco-rischi

- ⚠ Credito
- ⚠ Liquidità
- ⚠ Mercato
- ⚠ Rischi finanziari di banking book
- ⚠ Assicurativo
- ⚠ Strategico
- ⚠ Operativo
- ⚠ Reputazionale

## Struttura del sistema dei controlli interni



**Controlli di revisione interna**, volti ad individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente completezza, adeguatezza, funzionalità e affidabilità delle altre componenti del sistema dei controlli interni e del sistema informativo

**Controlli sui rischi e sulla conformità**, che hanno l'obiettivo di assicurare: la corretta attuazione del processo di gestione dei rischi; il rispetto dei limiti operativi assegnati alle varie funzioni; la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione

**Controlli di linea** di tipo gerarchico, sistematici e a campione che sono diretti ad assicurare il corretto svolgimento delle operazioni e che, per quanto possibile, sono incorporati nelle procedure informatiche; sono effettuati dalle stesse strutture operative e di business, anche attraverso unità dedicate a soli compiti di controllo, ovvero eseguiti nell'ambito del back office

# INDICE



Il rischio di non conformità nel sistema integrato di gestione dei rischi



**Il modello adottato da Intesa Sanpaolo**



Il contrasto agli illeciti e la collaborazione attiva con le Autorità



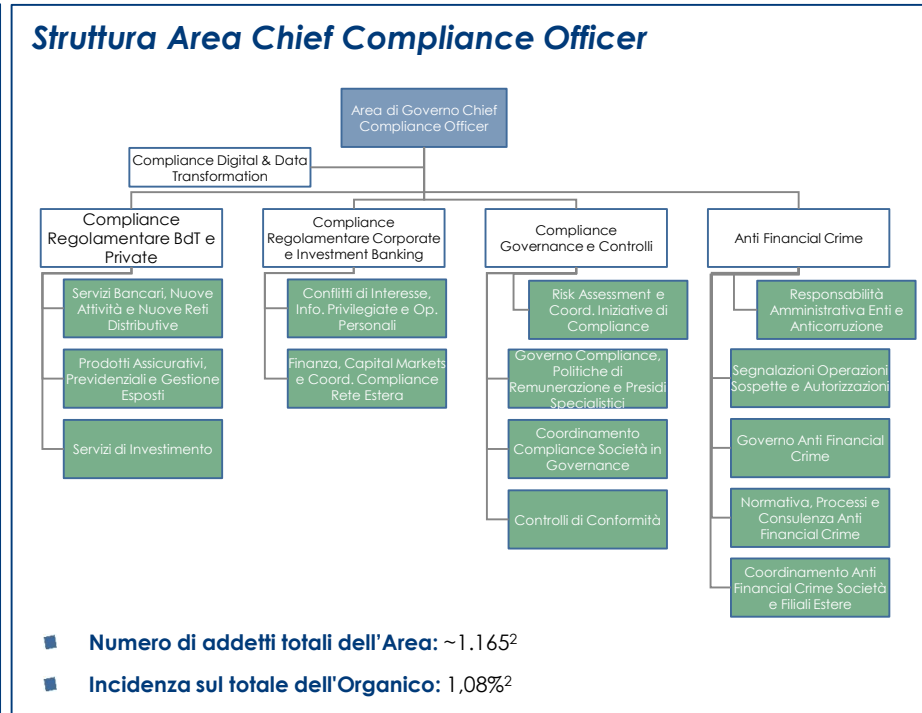
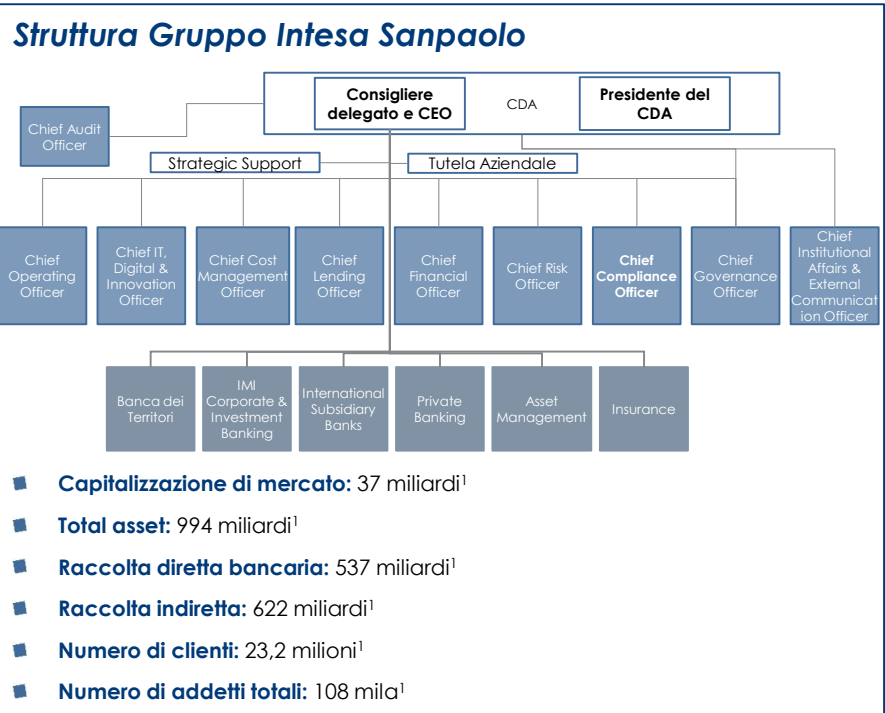
Le sfide future



Allegati

# La Funzione di conformità in Intesa Sanpaolo ...

Il rischio di non conformità alle norme è presidiato nel Gruppo Intesa Sanpaolo dall'**Area Chief Compliance Officer (CCO)**, collocata a diretto riporto del Chief Executive Officer



1. I dati comprendono anche le numeriche di UBI Banca; dati al 30 Giugno 2020, Capitalizzazione di mercato al 26 Novembre 2020  
 2. I dati comprendono anche gli addetti delle funzioni di conformità delle società controllate, inclusa UBI; dati al 30 Giugno 2020

## ... copre tutti gli ambiti normativi ....

L'Area CCO presidia la conformità alle norme sia direttamente, per gli ambiti per cui sussiste un'**indicazione regolamentare** in tal senso o per i quali si è reputata opportuna una **gestione accentrata**, sia indirettamente, tramite la **supervisione di strutture specialistiche** incaricate del presidio di conformità di singole norme (cd «**compliance graduata**»)

### Ambiti presidiati direttamente



- **Anti-Financial Crime:** antiriciclaggio, contrasto al finanziamento del terrorismo internazionale ed embarghi; anticorruzione; responsabilità Amministrativa degli enti
- **Compliance Regolamentare BdT & Private:** servizi di investimento; trasparenza; norme e iniziative a tutela della clientela; usura; sistemi di pagamento; intermediazione assicurativa e previdenziale
- **Compliance Regolamentare Corporate & Investment Banking:** normativa emittenti; market abuse; servizi di custody
- **Compliance Governance e Controlli:** sistemi di remunerazione e incentivazione; outsourcing

### Ambiti presidiati da funzioni specialistiche

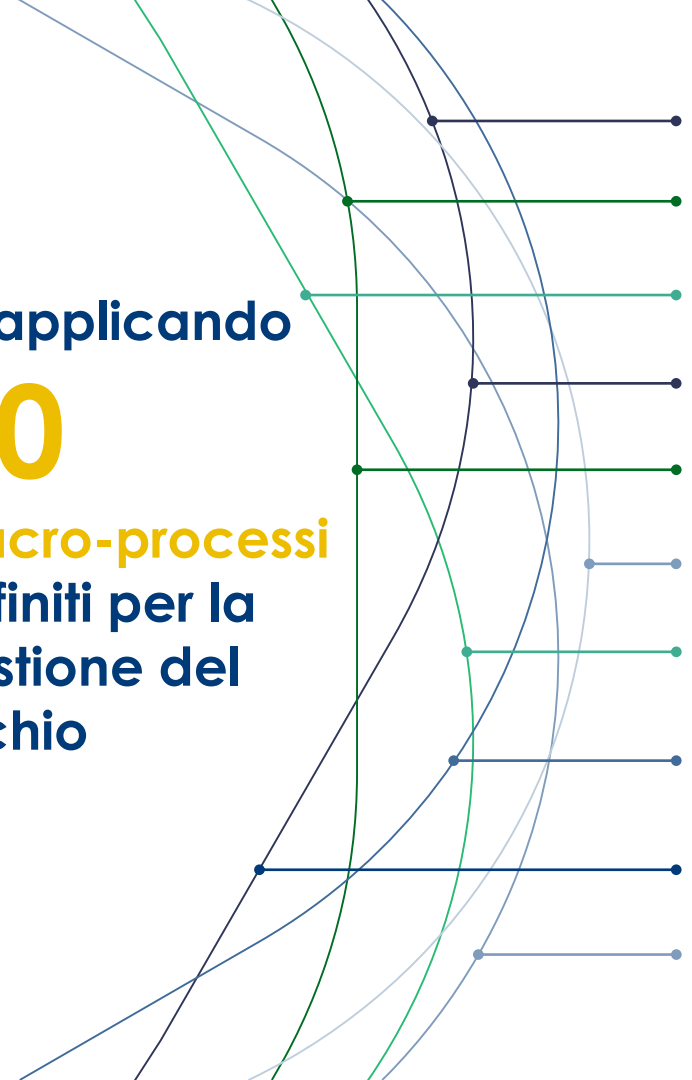


- Operazioni con parti correlate/soggetti collegati ed obbligazioni degli esponenti bancari
- Internal dealing/ Insider list proprietaria
- Organi sociali, governo societario e adempimenti societari
- Partecipazioni non finanziarie
- Procedure autorizzative di vigilanza e partecipazioni finanziarie
- Tutela della concorrenza
- Tutela della privacy
- Sicurezza sul lavoro
- Tutela ambientale
- Fiscale
- Giuslavoristico
- Sicurezza ICT
- Business Continuity
- Credito
- Acquisti
- Immobili
- Servizi a enti pubblici
- Pignoramenti
- Bilancio e vigilanza
- Codice etico e responsabilità sociale
- Informativa al pubblico

... applicando

10

macro-processi  
definiti per la  
gestione del  
rischio

- 
1. Definizione delle linee guida e delle regole metodologiche
  2. Risk assessment e risk appetite
  3. Programmazione delle attività
  4. Allineamento normativo
  5. Consulenza e clearing
  6. Assurance (controlli ex post)
  7. Diffusione della cultura di compliance
  8. Interazione con le Autorità e gestione degli eventi di non conformità
  9. Adempimenti specifici
  10. Flussi informativi agli organi societari



# Gli obiettivi dei macro-processi di gestione del rischio (1/3)

1.	<b>Definizione delle linee guide e delle regole metodologiche</b>	<ul style="list-style-type: none"><li>■ Definire le linee guida di riferimento e le regole metodologiche di presidio e di valutazione del rischio di non conformità a livello di Gruppo</li></ul>
2.	<b>Risk Assessment e Risk Appetite</b>	<ul style="list-style-type: none"><li>■ Identificare e valutare periodicamente i rischi di non conformità e le correlate vulnerabilità</li><li>■ Individuare gli interventi di rafforzamento dei presidi</li><li>■ Definire i principi di appetito al rischio, i conseguenti limiti e il monitoraggio periodico degli stessi</li></ul>
3.	<b>Programmazione delle attività</b>	<ul style="list-style-type: none"><li>■ Individuare le attività che si prevede di effettuare nell'esercizio - ripartite per macro-processo di compliance - declinate in termini di priorità, obiettivi, tempistiche e relativo assorbimento di risorse umane e finanziarie</li></ul>
4.	<b>Allineamento normativo</b>	<ul style="list-style-type: none"><li>■ Garantire che l'assetto complessivo dei processi e delle procedure aziendali risulti coerente con i requisiti previsti dalla normativa, sia esterna sia di autoregolamentazione</li></ul>

*Esempio in allegato*

## Gli obiettivi dei macro-processi di gestione del rischio (2/3)

### 5. Consulenza e clearing

- Prestare consulenza e assistenza agli Organi Societari e alle funzioni aziendali sull'interpretazione e sull'applicazione delle normative
- Valutare preventivamente la conformità alla normativa di: i) progetti innovativi, ivi inclusi l'avvio di nuove attività e l'inserimento in nuovi mercati, ii) nuovi prodotti e servizi da avviare alla commercializzazione e modifiche significative di prodotti esistenti, nel rispetto dei principi di product governance, iii) fattispecie e operazioni sensibili in relazione alle quali i processi aziendali prevedono una valutazione preventiva di conformità

### 6. Assurance (controlli ex post)

- Verificare ex post l'adeguatezza e l'effettiva applicazione dei processi e delle procedure per la gestione dei rischi di non conformità

### 7. Diffusione della cultura di compliance

- Garantire la diffusione a tutti i livelli aziendali di una cultura improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme che è un presupposto fondamentale per il presidio del rischio di non conformità, in particolare con riferimento ai rischi di condotta

## Gli obiettivi dei macro-processi di gestione del rischio (3/3)

8.	<b>Interazione con le Autorità e gestione degli eventi di non conformità</b>	<ul style="list-style-type: none"><li>■ Instaurare e mantenere nel continuo un rapporto proficuo con le Autorità e a garantire un'efficace gestione degli eventi di non conformità funzionale a ridurre i relativi rischi attraverso l'individuazione e l'implementazione degli opportuni interventi correttivi</li></ul>
9.	<b>Adempimenti specifici</b>	<ul style="list-style-type: none"><li>■ Svolgere le attività operative per la gestione di alcuni specifici adempimenti normativi (es. tenuta dei registri in materia di operazioni privilegiate e conflitti di interesse, segnalazioni in materia di antiriciclaggio e di market abuse)</li></ul>
10.	<b>Flussi informativi agli Organi Societari</b>	<ul style="list-style-type: none"><li>■ Garantire l'informativa verso gli Organi Societari circa l'adeguatezza dei presidi di conformità attraverso relazioni periodiche (semestrale e annuale) o ad evento</li></ul>

# INDICE



Il rischio di non conformità nel sistema integrato di gestione dei rischi



Il modello adottato da Intesa Sanpaolo



**Il contrasto agli illeciti e la collaborazione attiva con le Autorità**



Le sfide future



Allegati

# La Banca supporta le Autorità nel contrasto agli illeciti commessi da terzi in ambito Anti-Financial Crime (AFC) e Market Abuse

## Processi dedicati



Adeguata Verifica

- AFC  
 Market Abuse

Acquisire ed aggiornare nel continuo le **informazioni sulla clientela** per valutarne il rischio di riciclaggio ed applicare misure di mitigazione con approccio risk-based (e.g. adeguata verifica ordinaria e rafforzata)



Monitoraggio transazionale

- AFC  
 Market Abuse

Monitorare **tutte le operatività potenzialmente sospette** per individuare fenomeni di riciclaggio, manipolazioni di mercato ed episodi di insider trading, per segnalarli alle Autorità Competenti (UIF, Consob)



Embarghi

- AFC  
 Market Abuse

Impedire l'apertura di rapporti o l'effettuazione di pagamenti con **soggetti/ entità sottoposti a sanzioni finanziarie** da parte delle Autorità internazionali

## Esempi di strumenti utilizzati

- Calcolo di un **profilo di rischio** sulla base di più di 50 fattori
- Accesso a **database esterni** per arricchire le informazioni disponibili (e.g. notizie di stampa, soggetti con sentenze passate in giudicato, etc.)

- Utilizzo di **applicativi automatici di monitoraggio** che segnalano agli operatori potenziali operazioni anomale (ad esempio per importo, tipologia, tempistiche, soggetti coinvolti) sulla base di regole deterministiche

- Utilizzo di **applicativi automatici di monitoraggio** che confrontano le liste di soggetti sottoposti a sanzioni con l'anagrafe ed il sistema di pagamenti della Banca

Il sistema bancario impiega **risorse ingenti** (in investimenti in tecnologia e personale addetto ai controlli) per il contrasto del crimine finanziario – ad esempio, ad oggi Intesa Sanpaolo dedica al presidio delle tematiche AFC sul perimetro italiano circa 450 FTE<sup>1</sup> (incl. il coinvolgimento di responsabili di filiale, gestori e addetti alle funzioni di controllo di I e II livello).

In tale contesto, l'eccessiva numerosità di falsi positivi nell'attività di transaction monitoring dovrebbe portare ad un **confronto con il policy maker ed il regolatore** per evolvere gli attuali modelli di collaborazione attiva in un'ottica di maggiore efficacia ed efficienza.

# INDICE



Il rischio di non conformità nel sistema integrato di gestione dei rischi



Il modello adottato da Intesa Sanpaolo



Il contrasto agli illeciti e la collaborazione attiva con le Autorità



**Le sfide future**



Allegati

# Il futuro pone nuove importanti sfide alla funzione di conformità in ambiti quali la digitalizzazione, la ricerca di efficienza... <sup>14</sup>



## Digitalizzazione

- Per il presidio del rischio di non conformità, la funzione di compliance dovrà accompagnare la banca nella **trasformazione digitale dei processi di offerta a distanza** nonché di **lavoro a distanza**, con la valutazione dei rischi e l'individuazione dei presidi di conformità maggiormente integrati nei cd customer journey
- Dovrà inoltre sviluppare essa stessa **modalità digitalizzate di svolgimento delle proprie attività** soprattutto nelle aree ove sono necessarie soluzioni evolute di trattamento delle informazioni, in primis gli ambiti **Antiriciclaggio, Market abuse/Electronic communications surveillance**, ove le autorità attendono dai vigilati l'utilizzo di strumenti che sappiano cogliere tutte le opportunità offerte dalla tecnologia, a partire dalle soluzioni di intelligenza artificiale



## Ricerca di efficienza

- Oltre alla digitalizzazione, la ricerca di efficienza potrà essere attuata tramite **partnership con altri operatori in aree non competitive** per individuare sinergie di scopo, quali ad esempio le aree di collaborazione attività con le Autorità
- Da considerare altresì una riflessione circa le **sinergie di scopo** attivabili tra le attività di detection a fini Antiriciclaggio, ove riguardante operatività in strumenti finanziari, e Market abuse e quelle relative alle frodi
- In un contesto di crescente ricorso alle **esternalizzazioni di processi/attività aziendali**, sarà infine necessario un adeguato presidio dei relativi aspetti di conformità

# ... l'internazionalizzazione ed i temi Environmental Social Governance



Internazionalizzazione

- I prevedibili **processi di integrazione europea** richiedono una accresciuta dimensione internazionale della compliance, delle sue risorse, dei suoi modelli operativi e delle sue soluzioni tecnologiche
- La funzione di compliance dovrà inoltre gestire le conseguenze derivanti dall'annunciata volontà espressa dalla Commissione UE di accentrare presso un supervisore europeo il **presidio dell'Antiriciclaggio**



Environmental Social Governance

- I **temi ESG (Environmental Social Governance)**, impattando l'intera organizzazione, dovranno essere oggetto di attento presidio anche da parte della funzione di conformità
- In tale ambito, sarà necessario agire il **ruolo della compliance rispetto ai rischi climatici e ambientali**, assicurando il presidio dei rischi di responsabilità legale e la loro integrazione in tutti i processi rilevanti, in stretto coordinamento con il risk management, coerentemente con le recenti linee guida di BCE



# Le sfide future vanno affrontate sfruttando le opportunità offerte dall'evoluzione tecnologica...



## Maggiore efficacia degli algoritmi

E.g. con l'evoluzione da logiche deterministiche a modelli di «machine learning», che abilitano il computer ad imparare a partire dall'esperienza o da input esterni



## Valorizzazione dei dati disponibili

Grazie alla disponibilità di una maggiore capacità di storicizzazione delle informazioni disponibili ed all'evoluzione della capacità computazionale degli applicativi utilizzati



## Nascita di nuovi partner tecnologici

Le «**RegTech**», che offrono soluzioni tecnologiche evolute per assistere gli operatori bancari nel presidio del rischio, e le «**SupTech**», sviluppate dalle Autorità per le potenziare le proprie attività di supervisione

# ... e valorizzando le Persone come più importante fattore abilitante per la trasformazione



## Investimento sulle persone

Nonostante le grandi potenzialità delle tecnologie disponibili, l'evoluzione digitale della Compliance non può realizzarsi senza un **forte investimento sulle persone** che presidiano i processi di conformità



## Mix di competenze

La principale sfida di affrontare è la necessità di **arricchire il mix di competenze** delle risorse delle funzioni di Compliance degli intermediari finanziari favorendo la diffusione di «skill digitali» e nuovi modi di lavorare, tramite l'acquisizione di nuove competenze e la **creazione di nuovi percorsi professionali**



## Collaborazione con il territorio

Sarà altresì strategico sviluppare collaborazioni con Università e Regtech, che valorizzino le **competenze presenti sul territorio**

# INDICE



Il rischio di non conformità nel sistema integrato di gestione dei rischi



Il modello adottato da Intesa Sanpaolo



Il contrasto agli illeciti e la collaborazione attiva con le Autorità



Le sfide future



**Allegati**

# Esempio: Intesa Sanpaolo svolge annualmente un Risk Assessment Anti-Financial Crime secondo una metodologia coerente con le linee guida di Banca d'Italia

## Elementi della metodologia di Risk Assessment

Rischio inerente

- 5 categorie di risk factor
  - Geografia, clienti e intermediari, prodotti e servizi, canali di distribuzione, transazioni
- 28 Key Risk Indicator

Vulnerabilità

### Sezione Qualitativa

- 39 domande (punteggio da 1 a 4)
  - Media tra punteggio Antiriciclaggio ed Embarghi

### Sezione Quantitativa

- 13 Key Process Indicator suddivisi lungo 3 pilastri della vulnerabilità

Rischio residuo

Valutazione dell'esposizione al rischio di ogni linea di business, secondo una scala di quattro valori, sulla base della combinazione dei giudizi di rischio inerente e di vulnerabilità all'interno di una matrice

