Compliance Policy

Consiglio di Amministrazione del 29 marzo 2023

INDICE

1 Premessa

Scopo del presente documento è fornire una descrizione dei principi adottati da Banca Mediolanum S.p.A. in tema di gestione del rischio di non conformità e delle modalità di recepimento di tali principi all'interno del complessivo framework metodologico adottato dalla Funzione.

1.1 CONTESTO DI RIFERIMENTO

L'evoluzione continua dei mercati finanziari, in termini di innovazione dei prodotti, di trasferimento del rischio e di proiezione internazionale, rende sempre più complessi l'identificazione ed il controllo dei comportamenti che possono dar luogo a violazioni di norme, di standard operativi, di principi deontologici ed etici dell'attività bancaria. Il rischio di non conformità alle norme, definito come il *"rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative o di autoregolamentazione*", è diffuso a tutti i livelli dell'organizzazione aziendale.

Per questo motivo, è richiesto agli intermediari di dotarsi di articolati sistemi di controllo interno e specifici presidi organizzativi - tra i quali la Funzione Compliance - volti ad assicurare il rispetto, non solo formale ma anche sostanziale, delle prescrizioni normative e di autoregolamentazione applicabili, promuovendo allo stesso tempo al loro interno una cultura aziendale improntata a principi di onestà e correttezza.

Un'efficace attività di prevenzione dei rischi di non conformità non può essere demandata alle sole funzioni di controllo, ma deve svolgersi, in primo luogo, dove il rischio viene generato, in particolare nell'ambito delle linee operative, le quali sono le prime responsabili del processo di gestione dei rischi; nel corso dell'operatività di competenza, tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi.

Nell'ottica di assicurare un'efficace prevenzione dei rischi di non conformità alla normativa, è inoltre fondamentale che le diverse strutture aziendali assicurino il tempestivo coinvolgimento della Funzione Compliance nella valutazione *ex ante* della conformità alla regolamentazione applicabile di tutti i progetti innovativi tra cui assumono particolare rilievo quelli inerenti ai nuovi prodotti e servizi da commercializzare o distribuire o inerenti alle modifiche al sistema premiante aziendale.

1.2 OBIETTIVI DEL DOCUMENTO

Banca Mediolanum S.p.A. riconosce che la promozione di una cultura aziendale basata su principi di onestà, correttezza e rispetto delle norme a tutti i livelli dell'organizzazione contribuisce alla creazione di valore, così come la reputazione aziendale è un valore imprescindibile alla base del rapporto fiduciario con la clientela e della propria credibilità verso il mercato e verso gli *stakeholder.* La Funzione Compliance presiede, secondo un approccio *risk based* ed in coerenza con il principio di proporzionalità, alla gestione del rischio di non conformità con riferimento all'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio. Il nostro ordinamento, infatti, prevede un sistema di regole che, indicando principi di

carattere generale, integrati da linee guida applicative, "best practices" e prassi largamente diffuse e accettate, assegna agli intermediari il ruolo di determinare, in funzione del loro modello di business e della loro dimensione operativa, le soluzioni organizzative più idonee a garantire una sana e prudente gestione. Ciò consente agli intermediari di focalizzarsi con maggiore efficacia, in relazione alla propria dimensione e complessità organizzativa e di business, sulle aree con profili di rischio più significativi modulando di conseguenza le attività di controllo.

A tal fine, viene emanato il presente documento che fornisce le linee di indirizzo ed identifica i requisiti da rispettare per la definizione del modello di controllo sul rischio di non conformità e per la corretta gestione (articolata nelle fasi di progettazione, realizzazione e manutenzione) di un modello di controllo su tale rischio (nel seguito del documento anche "modello di compliance") di cui Banca Mediolanum S.p.A. si dota.

In particolare, questo documento, che è parte integrante della normativa interna della Banca, definisce le linee guida relativamente alle:

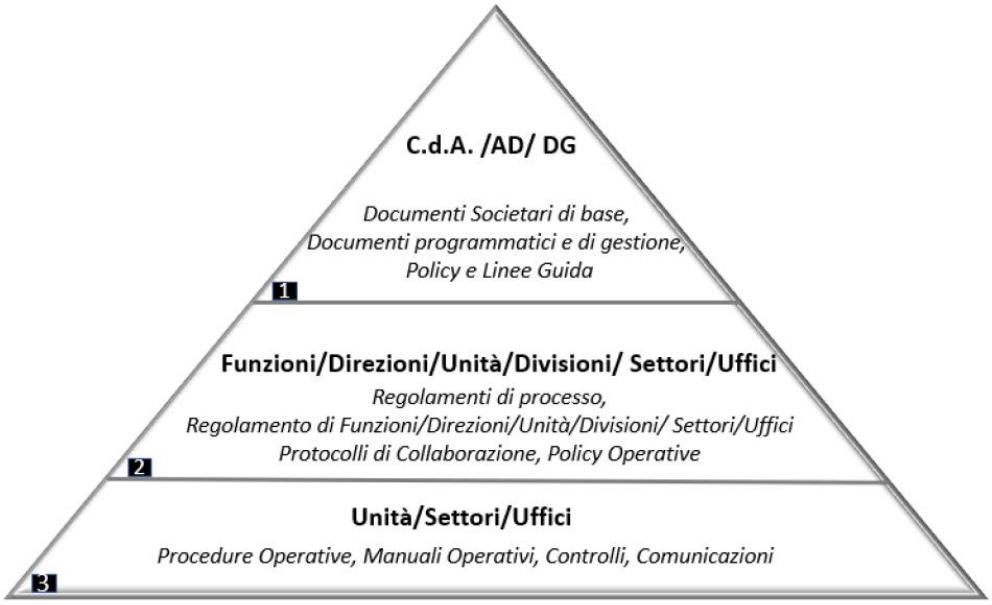
- regole di governo e politiche di gestione dei rischi di non conformità da adottare;
- modalità di gestione del rischio di non conformità e, a tal fine:
    - identifica il perimetro delle norme applicabili ai fini della mappatura dei rischi di non conformità a cui sono esposti i processi aziendali;
    - descrive il processo di *compliance* adottato;
    - descrive il *framework* definito per le verifiche di adeguatezza e di funzionamento;
    - descrive il modello di collaborazione esistente tra le diverse funzioni coinvolte nel presidio dei rischi di *compliance*;
    - identifica i ruoli e le responsabilità delle unità organizzative coinvolte nella gestione del rischio di non conformità.

La Funzione di Compliance, in tale contesto, svolge le proprie attività secondo le linee guida sopra riportate e in coerenza con le normative tempo per tempo applicabili[1] adottando, con particolare riguardo ai processi distributivi della Banca, un approccio *end-to-end*. In tale ottica, in coerenza con le previsioni normative introdotte nel tempo nell'ambito della *product governance*, la Funzione di Compliance svolge un'attività di valutazione ex ante dei nuovi prodotti e servizi e delle modifiche sostanziali agli stessi, siano essi bancari, assicurativi o di investimenti, ai processi e ai sistemi esistenti.

Con riferimento alla "*Policy di Conglomerato sulle modalità di redazione, aggiornamento, approvazione e diffusione della Normativa Interna*", il presente documento si colloca al primo livello della piramide documentale richiamata nello schema seguente.

Modello della normativa interna di riferimento

[1] In relazione al contesto normativo di riferimento si rimanda a quanto indicato nel paragrafo 6 della presente Policy in cui sono indicati i principali riferimenti normativi e regolamentari in tema di gestione del rischio di non conformità.



2 Applicabilità

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Banca Mediolanum S.p.A., nell'ambito dei compiti ad esso affidati dalla normativa di vigilanza sul Sistema dei Controlli Interni. Nella sua veste di Capogruppo, detto documento è conseguentemente inviato per l'adozione, secondo un principio di proporzionalità e tenuto conto delle normative e specificità locali, ivi comprese le caratteristiche delle attività di business, agli Organi con funzione di supervisione strategica delle Società facenti parte del Gruppo Bancario Mediolanum.

Il documento viene inoltre trasmesso a Mediolanum Vita, Capogruppo del Gruppo assicurativo Mediolanum, affinché indirizzi le metodologie del Gruppo assicurativo in coerenza a quanto definito da Banca Mediolanum in qualità di impresa madre del Conglomerato Finanziario.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del documento sono deliberati dal Consiglio di Amministrazione della Società, su proposta della Funzione Compliance.

3 Definizioni

Compliance Risk: specifico adempimento richiesto da una determinata normativa, per non incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di

violazioni di norme imperative (leggi, regolamenti) o di autoregolamentazione (ad esempio codice di condotta, codice di autodisciplina).

Controlli di linea (c.d. "controlli di primo livello"): l'insieme dei controlli diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (ad es., controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo o presidio che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del *back office*; per quanto possibile, essi sono incorporati nelle procedure informatiche.

Controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello")**,** l'insieme dei controlli che hanno l'obiettivo di assicurare, tra l'altro:

- la corretta attuazione del processo di gestione dei rischi;
- la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.

Le funzioni preposte a tali controlli sono distinte da quelle operative; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi.

DPO (Data Protection Officer): Unità di Supporto Manageriale, all'interno della quale opera il Responsabile della Protezione dei Dati ("Data Protection Officer" o "DPO") nominato dal Titolare del trattamento dei dati in conformità al Regolamento Europeo 2016/679 in materia di protezione dei dati personali ("General Data Protection Regulation" o "GDPR").

Funzioni Aziendali di Controllo: la Funzione di conformità alle norme (*Compliance*), la Funzione di controllo dei rischi (*Risk Management*), la Funzione deputata a prevenire e contrastare i fenomeni nonché la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo (Antiriciclaggio), la Funzione di revisione interna (*Internal Auditing*).

Funzione Compliance*:* Funzione di secondo livello a cui è affidato il compito specifico di presiedere, secondo un approccio *risk based*, alla gestione del rischio di non conformità con riguardo all'attività aziendale, verificando che le procedure siano adeguate a prevenire tale rischio, consistente nella violazione di norme di etero regolamentazione (leggi e regolamenti) ed autoregolamentazione (codici di condotta e codici etici) applicabili alla Società. Detta Funzione è parte integrante del Sistema dei Controlli Interni.

Funzioni di Controllo: le Funzioni Aziendali di Controllo, il Dirigente Preposto, il Revisore Legale dei Conti, l'Organismo di Vigilanza istituito ai sensi del D.lgs. 231/01 e il Data Protection Officer.

Organi aziendali*:* il complesso degli Organi con funzioni di supervisione strategica, di gestione e di controllo. La funzione di supervisione strategica e quella di gestione attengono, unitariamente, alla gestione dell'impresa e possono quindi essere incardinate nello stesso Organo aziendale.

Organo con funzione di controllo*:* organo che verifica la regolarità dell'attività di amministrazione e l'adeguatezza degli assetti organizzativi e contabili della Società (ruolo svolto dal Collegio Sindacale nella Capogruppo e nelle società controllate italiane).

Organo con funzione di supervisione strategica*:* organo aziendale al quale – ai sensi del Codice civile o per disposizione statutaria – sono attribuite funzioni di indirizzo della gestione d'impresa, mediante, tra l'altro,

esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche della Società (ruolo attribuito al Consiglio di Amministrazione).

***Organo con funzione di gestione**:* organo aziendale o componenti di esso ai quali – ai sensi del Codice civile o per disposizione statutaria – spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica (ruolo attribuito all'Amministratore Delegato). Il Direttore Generale, insieme all'Amministratore Delegato, rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione.

Revisione interna (c.d. "controlli di terzo livello"): attività volta a individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del Sistema dei Controlli Interni e del sistema informativo (*ICT audit*), con cadenza prefissata in relazione alla natura ed all'intensità dei rischi.

Risk appetite: livello di rischio (complessivo e per tipologia) che la Società intende assumere per il perseguimento dei suoi obiettivi strategici.

Risk Appetite Framework – RAF: quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il business model e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli.

Rischio inerente: nella logica del c.d. rischio "potenziale", la probabilità per la Società di subire un danno diretto od indiretto di natura sanzionatoria, penale, finanziaria o reputazionale senza considerare l'organizzazione ed il funzionamento dei propri presidi organizzativi ed il più generale Sistema dei Controlli Interni.

Rischio residuo: giudizio di sintesi che tiene conto degli esiti delle verifiche di adeguatezza e di funzionamento dei presidi organizzativi in essere.

Sezione della normativa (Compliance Risk): insieme omogeneo di argomenti di una specifica normativa di fonte primaria o secondaria, da cui discende un *compliance risk.*

Sistema dei Controlli Interni: l'insieme delle regole, delle procedure delle strutture organizzative, volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

Unità Specialistica di compliance (anche "Unità Specialistica"): l'unità organizzativa, che nell'ambito del modello di compliance adottato dalla Banca è riconosciuta idonea, in quanto dotata di adeguate competenze tecnico-specialistiche e professionalità, al presidio decentrato di ambiti normativi specifici, svolgendo attività specificatamente attribuite, come meglio definito nel seguito del presente documento.

Strutture Operative: tutte le restanti unità organizzative previste dall'Ordinamento dei Servizi, diverse dalle Funzioni di controllo e dalle Unità Specialistiche di *compliance.*

4 Ruoli e responsabilità

4.1 PRINCIPI ORGANIZZATIVI E RUOLI DEGLI ORGANI SOCIALI

Il modello di compliance viene approvato dagli Organi Aziendali che definiscono compiti e responsabilità in materia di conformità tramite apposita regolamentazione interna.

Per quanto riguarda Banca Mediolanum S.p.A., la responsabilità dello sviluppo e della gestione della politica di conformità è affidata al Responsabile della Funzione Compliance, nella terminologia corrente denominato anche "**Compliance Officer di Gruppo" (in breve COG)**, cui spetta, inoltre, il compito di sviluppare attività di coordinamento con le omologhe funzioni delle società del Gruppo, nell'ambito delle politiche di conformità adottate a livello di Gruppo Bancario.

Limitatamente ai casi previsti dalla regolamentazione secondaria, ogni Società del Gruppo identifica e nomina un **"Compliance Officer delle Società controllate" (in breve CO)**, che, per quanto attiene alle società italiane del Gruppo. viene nominato da parte dell'organo aziendale competente ed è responsabile della attuazione del modello di *compliance* all'interno della propria realtà aziendale.

Nelle Società estere per le quali la normativa locale prevede tale figura e, comunque, in ottemperanza a quanto richiesto dalle disposizioni regolamentari locali, viene designato un **"Compliance Officer Estero" (in breve COE)** al fine di assicurare una corretta gestione del rischio derivante dalla necessità di rispettare tutte le disposizioni applicabili anche in relazione ai diversi ambiti di operatività internazionale.

Temporanea assenza del Compliance Officer

Per disciplinare le ipotesi di assenza od impedimento del COG, Banca Mediolanum si è dotata della "*Policy per la nomina, rimozione e sostituzione dei Responsabili delle Funzioni aziendali di Controllo*" attraverso la quale sono descritti i principi relativi alla nomina, rimozione e sostituzione dei Responsabili delle Funzioni aziendali di Controllo di Banca Mediolanum S.p.A.

Nei casi indicati nella suddetta Policy per la gestione della temporanea sostituzione del Compliance Officer di Gruppo, la Funzione prevede che, nel periodo di assenza temporanea[2], per il perimetro di Banca Mediolanum, le responsabilità e le attività siano di competenza del Responsabile Advisory & Controls Banca.

In caso invece di assenza temporanea del Compliance Officer delle società controllate, salvo differente valutazione del Consiglio di amministrazione delle stesse, le responsabilità e le attività sono temporaneamente affidate al Compliance Officer di Gruppo.

[2] Per assenza temporanea si rimanda a quanto previsto nel par. 5.5 della "Policy per la nomina, rimozione e sostituzione dei Responsabili delle Funzioni aziendali di Controllo".

Accordi di esternalizzazione

In considerazione del modello di *compliance* adottato, le Società italiane del Gruppo Bancario possono, previa valutazione, sottoscrivere accordi di servizio con Banca Mediolanum S.p.A. aventi ad oggetto l'esternalizzazione di attività svolte dalla Funzione di conformità alle norme. L'esternalizzazione avviene nel rispetto della regolamentazione di Vigilanza, in conformità ai principi sanciti all'interno della "Politica aziendale in materia di esternalizzazione" e deve risultare formalizzata in uno specifico accordo di prestazione di servizi.

4.2 UNITÀ ORGANIZZATIVE COINVOLTE NELLA GESTIONE DEL RISCHIO DI NON CONFORMITÀ

Il modello adottato per il presidio del rischio di non conformità (cd. modello di *compliance)* prevede:

- la responsabilità in capo alla **Funzione Compliance**;
- l'individuazione di **Unità Specialistiche** incaricate di garantire l'adeguato presidio di specifici ambiti normativi a cui sono attribuite determinate fasi del processo di *compliance,* come di seguito illustrato;
- l'attribuzione alle altre **Funzioni Aziendali di Controllo** della responsabilità degli ambiti normativi alle stesse demandati *ex lege,* riferendo direttamente agli Organi Aziendali competenti.

La Funzione Compliance può avvalersi in ogni caso del supporto di risorse appartenenti ad unità organizzative che, ancorché in assenza di delega e/o di costituzione di una specifica Unità Specialistica, dispongano al loro interno di competenze tecniche idonee a supportarla nell'approfondimento di specifiche tematiche. Tale supporto, dovuto qualora richiesto, può avere ad oggetto in particolare l'analisi di dettaglio delle novità normative, l'identificazione dei rischi e la definizione dei macro interventi di adeguamento.

4.2.1 FUNZIONE COMPLIANCE

La Funzione Compliance presiede alla gestione dei rischi di non conformità alle norme, secondo un approccio *risk based*, con riguardo all'attività aziendale, avvalendosi, per il presidio di determinati ambiti normativi per cui sono previste forme di presidio specializzato, di Unità Specialistiche appositamente individuate nella Compliance Policy, cui sono attribuite determinate fasi del processo di compliance. Come, peraltro, statuito dalla normativa di riferimento – la Circolare 285/13 di Banca d'Italia – "*con riferimento ad altre normative per le quali siano già previste forme specifiche di presidio, la banca, in base a una valutazione dell'adeguatezza dei controlli specialistici a gestire i profili di rischio di non conformità, può graduare i compiti della compliance, che comunque è responsabile, in collaborazione con le funzioni specialistiche incaricate, almeno della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità*".

Alla Funzione competono attività di consulenza specialistica, ai fini della valutazione del rischio di conformità, il costante monitoraggio del contesto normativo esterno (alert normativo), la valutazione dell'impatto delle normative (*gap analysis*) sui processi aziendali, le verifiche di adeguatezza (attraverso l'identificazione di proposte di modifiche, anche organizzative e procedurali, derivanti anche da *gap analysis*, valutazioni e pareri)

e di funzionamento di assetti e processi aziendali atte a prevenire la violazione di norme imperative o di auto-regolamentazione e il monitoraggio dell'adozione delle misure correttive proposte.

Con riferimento a quanto previsto esplicitamente dalla normativa, la Funzione Compliance è chiamata a svolgere i seguenti adempimenti:

- ausilio alle strutture aziendali per la valutazione dei rischi di non conformità alle norme;
- valutazione di idonee procedure per la prevenzione del rischio rilevato, con possibilità di richiederne l'adozione e la verifica della loro adeguatezza e corretta applicazione;
- verifica del funzionamento degli adeguamenti organizzativi suggeriti per la prevenzione del rischio di non conformità alle norme;
- identificazione nel continuo delle norme applicabili alla banca e misurazione/valutazione del loro impatto sui processi e procedure aziendali, ivi comprese le misure da adottare per garantire la conformità a leggi, norme, regolamenti e standard applicabili;
- proposta di modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati;
- predisposizione di flussi informativi diretti agli organi aziendali e alle strutture coinvolte, fermo restando l'obbligo di rispondere tempestivamente agli organi medesimi in caso di richiesta di informazioni e consulenza.

Il modello adottato per il presidio del rischio di non conformità prevede pertanto un presidio diretto in capo alla Funzione Compliance per le norme più rilevanti ai fini del rischio di non conformità, quali quelle che riguardano l'esercizio dell'attività bancaria e di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e, più in generale, la disciplina posta a tutela del consumatore, e per quelle norme per le quali non siano previste forme di presidio specializzato all'interno della Banca (c.d. Unità Specialistiche) ovvero non rientrino nel perimetro di competenza di altre Funzioni Aziendali di Controllo.

Per quanto attiene al presidio decentrato assicurato dalle Unità Specialistiche, la Funzione Compliance è responsabile di valutare l'adeguatezza di tale presidio al rischio di non conformità.

Allo scopo di assicurare un'efficace gestione del rischio di non conformità, la Funzione Compliance soddisfa i requisiti di seguito riportati.

Indipendenza

Per svolgere in modo appropriato i propri compiti, la Funzione Compliance deve essere indipendente, in termini di *collocazione* organizzativa ed imparzialità.

L'assetto organizzativo della Funzione deve essere tale da assicurarne l'efficacia, al riguardo:

- il Responsabile:
  - riveste un ruolo all'interno della Società tale da conferire autorevolezza alla Funzione di controllo;
  - è collocato in posizione-gerarchico funzionale adeguata alle dirette dipendenze dell'Organo con funzione di gestione o dell'Organo con funzione di supervisione strategica;
  - ha accesso a tutti i necessari documenti aziendali per potere adempiere ai propri compiti previsti dalla regolamentazione di Vigilanza;

- non deve avere responsabilità dirette od anche indirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree. In generale, non deve essere gerarchicamente subordinato ai responsabili delle funzioni sottoposte a controllo;
- riferisce direttamente agli Organi aziendali con accesso diretto all'Organo con funzione di supervisione strategica, all' Organo di Gestione ed all'Organo con funzione di controllo e comunica con essi senza restrizioni o intermediazioni;
- deve disporre di un budget autonomo ed adeguato alla pianificazione e la gestione dei propri interventi;

- i membri della Funzione Compliance devono essere in una posizione sufficientemente indipendente da poter manifestare il proprio giudizio, esprimere pareri e fornire raccomandazioni in modo imparziale. Indipendentemente dal proprio inquadramento all'interno dell'organizzazione, devono essere scevri da qualsiasi effettivo conflitto di interesse derivante da relazioni professionali o personali o interessi pecuniari o di altro tipo, che potrebbero contrastare con i doveri ai quali sono sottoposti. Inoltre, gli stessi devono essere immuni da indebite interferenze che possono limitare o modificare la loro sfera d'azione o lo svolgimento delle proprie funzioni o ancora che possano intaccare o influenzare significativamente il loro giudizio ovvero il contenuto del proprio lavoro. Inoltre, i membri delle funzioni di controllo non possono essere contemporaneamente impiegati in altre attività che potrebbero essere in conflitto con il proprio ruolo. Ove si verificasse una delle situazioni sopra delineate, queste devono essere rappresentate in modo chiaro al responsabile della Funzione Compliance, per permettere allo stesso di rimuovere le cause che possono limitare l'indipendenza dei componenti la Funzione.

.

Risorse adeguate e formazione

L'efficacia della Funzione Compliance dipende dalla qualità, dalla formazione e dall'esperienza dei membri della Funzione. È necessario, pertanto, assicurare un adeguato dimensionamento quali-quantitativo delle risorse, disponendo al proprio interno di persone con idonee qualità personali che possiedano adeguate conoscenze normative, del modello di *business* e dei prodotti o siano comunque in grado di sviluppare tali conoscenze e qualità. La formazione deve essere personalizzata sulle necessità individuali, deve essere sia teorica (su normativa e prodotti) che pratica. La formazione, anche mediante adeguate modalità di autoformazione, deve essere continua, ben pianificata e diretta anche a tutto il personale interessato.

Risorse tecnologiche

La complessità delle aree di *business* in cui opera la Società e la presenza di specifici requisiti normativi cui occorre uniformarsi, rendono necessario l'utilizzo di strumenti informativi e tecnologici a supporto delle Funzioni di controllo. Al riguardo, la Banca assicura che dette risorse tecnologiche siano fruibili, coprano tutte le aree di *business* e fungano da supporto, in particolare, alla Funzione Compliance.

4.2.2 UNITÀ SPECIALISTICHE

Le Unità Specialistiche incaricate di garantire l'adeguato presidio degli ambiti normativi di competenza, sono responsabili dello svolgimento di specifiche attività nell'ambito del processo di adeguamento normativo relativamente alle tematiche di rispettiva competenza.
Le Unità Specialistiche individuano al loro interno specifici Referenti i quali provvedono all'aggiornamento della regolamentazione interna afferente all'ambito normativo di propria competenza.

Nell'ottica di ricondurre ad unità il processo di gestione del rischio di non conformità, favorendo lo sviluppo da parte della Funzione Compliance di una visione d'insieme della rischiosità aziendale, le Unità Specialistiche attivano regolari flussi informativi verso la Funzione medesima, secondo le modalità ed il *template* fornito ("Questionario di Attestazione"), ove attestano, attraverso un set di domande e risposte, le attività svolte nel periodo di riferimento sugli ambiti normativi di rispettiva competenza.

4.2.3 FUNZIONI AZIENDALI DI CONTROLLO

Nel modello di *compliance* adottato, va precisato il ruolo svolto dalle Funzioni Aziendali di Controllo, diverse dalla Compliance, le quali garantiscono un presidio strutturato e puntuale, sulla base di procedure consolidate, delle normative attribuite al loro ambito di intervento *ex lege*.
La collaborazione tra le altre Funzioni Aziendali di Controllo e la Funzione Compliance trova attuazione nello scambio di regolari flussi informativi anche in occasione delle periodiche riunioni di coordinamento delle Funzioni di Controllo e anche nell'eventuale partecipazione al Comitato Rischi da parte delle stesse, in linea e nel rispetto di quanto definito dalle Linee Guida e Principi base di Coordinamento di Gruppo tra Organi e Funzioni di controllo.

4.2.4 ALTRE UNITÀ ORGANIZZATIVE

A fronte di un adeguato presidio del rischio di non conformità, tutte le unità organizzative sono coinvolte nel processo in esame; sono dunque richiesti alcuni specifici requisiti comportamentali a ciascun membro delle stesse.
Poiché il rischio di non conformità alle norme è diffuso a tutti livelli dell'organizzazione aziendale, soprattutto nell'ambito delle linee operative, l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato; è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale al fine di limitare gli eventi il cui accadimento genera o può generare come effetto:

- una perdita finanziaria derivante dall'irrogazione di sanzioni pecuniarie o dall'obbligo di risarcire danni a seguito di comportamenti non conformi alle disposizioni di legge;
- una flessione degli utili o del valore della Società derivante da difficoltà operative connesse al non tempestivo adeguamento alle norme, e quindi una percezione negativa dell'immagine dell'azienda da parte degli *stakeholders* (clienti, collaboratori, controparti, azionisti, investitori, Autorità di Vigilanza, etc.).

Responsabili

Ogni Responsabile di unità organizzativa è tenuto a curare al meglio la gestione del personale e degli strumenti operativi allo stesso affidati per assicurare il costante perseguimento degli obiettivi aziendali e deve, per quanto di competenza, osservare e far rispettare scrupolosamente tutte le norme vigenti, sia di legge che quelle emanate dalla società di appartenenza. A ciascun Responsabile è attribuita la responsabilità complessiva della conformità all'interno della propria struttura. Allorché i Responsabili, nell'espletamento delle proprie funzioni, rilevino che i processi operativi non siano aderenti alle norme di riferimento, devono, previ i necessari approfondimenti, interessare senza ritardi, la Funzione Compliance per l'espletamento delle attività di competenza.

Dipendenti e altri Collaboratori

Tutti i Dipendenti ed i Collaboratori, nell'ambito delle mansioni a cui sono assegnati, sono tenuti a conoscere ed uniformarsi alle leggi, ai regolamenti ed alle norme emanate dalla propria Società di appartenenza. Allorché Dipendenti e Collaboratori, nell'espletamento delle proprie attività, rilevino che i processi operativi non siano aderenti alle norme di riferimento, devono darne tempestiva comunicazione al proprio Responsabile. I documenti aziendali che disciplinano aspetti organizzativi e comportamentali afferenti al rispetto delle norme vigenti, sia di legge che quelle emanate dalla Società di appartenenza, sono portati a conoscenza di tutti i Dipendenti e dei Collaboratori attraverso la loro pubblicazione e diffusione secondo le modalità previste.

Consulenti Finanziari

I Consulenti Finanziari, o comunque i soggetti che operano sulla base di un mandato di agenzia, nell'ambito delle attività svolte per conto della Società con cui collaborano, sono tenuti a conoscere e uniformarsi alle leggi, ai regolamenti ed alle norme emanate dalla Società stessa. I documenti aziendali che disciplinano aspetti organizzativi e comportamentali afferenti al rispetto delle norme vigenti, sia di legge che quelle emanate dalla società di appartenenza, sono portati a conoscenza dei Consulenti Finanziari attraverso la loro pubblicazione con le modalità di diffusione previste.

5 Principi in tema di gestione del rischio di non conformità

5.1 TASSONOMIA DEI RISCHI

Il rischio di non conformità alle norme è definito come *"il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina)[3]".*

La Funzione di conformità alle norme presiede, secondo un approccio *risk based*, alla gestione del rischio di non conformità con riguardo all'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio, secondo le modalità più oltre illustrate.

5.2 SIGNIFICATIVITÀ DEL RISCHIO

Il Sistema dei Controlli Interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento di diverse finalità tra cui il contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca - *Risk Appetite Framework* - "RAF".

L'Organo con funzione di supervisione strategica determina la significatività del rischio quale manifestazione della propria soglia di tolleranza al rischio, in coerenza con il *business model* ed il piano strategico, le politiche di governo dei rischi nonché i relativi processi di riferimento.

5.3 MODALITÀ DI GESTIONE

Spetta alla Funzione Compliance l'identificazione, con periodicità almeno annuale, del quadro normativo applicabile e rilevante per la Società, nonché il presidio nel continuo di tale perimetro normativo individuato.

Ai fini di una gestione efficace del rischio di non conformità, è quindi fondamentale definire e mantenere regolarmente aggiornato il perimetro delle norme applicabili alla Società e valutare l'adeguatezza dei presidi in essere (c.d. *Rule Map*).

In particolare, sono individuate:

- normative incluse nel "perimetro accentrato", ovvero le normative per le quali la regolamentazione già prevede una stretta competenza della Funzione Compliance, come ad esempio, per quelle connesse all'esercizio dell'attività bancaria e di intermediazione, alla gestione dei conflitti di interesse, alla trasparenza nei confronti della clientela e, più in generale, alla disciplina posta a tutela del consumatore;
- normative incluse nel "perimetro decentrato" o "indiretto", ovvero le altre normative, il cui presidio può essere assicurato in relazione a specifiche attività del processo di Compliance dalle Unità Specialistiche

[3] Circolare n. 285 del 17 dicembre 2013 e successivi aggiornamenti.

attraverso una fattiva interazione ed un costante coordinamento con la Funzione Compliance. L'attribuzione del presidio di talune normative alle Unità Specialistiche costituisce una scelta da adottare in fase di definizione o aggiornamento del "quadro normativo" di riferimento.

Si fa infine presente che sono escluse dal perimetro accentrato e "indiretto" di competenza della Funzione di Compliance, quelle normative che sono presidiate da altre Funzioni di Controllo quali principalmente, la vigilanza prudenziale e Resolution Recovery Plan, di competenza della Funzione Risk Management, la normativa Antiriciclaggio, di competenza della Funzione Antiriciclaggio, nonché la normativa sulla Privacy, di Competenza del Data Protection Officer (DPO).

Al fine di garantire uniformità nella gestione del rischio di non conformità da parte delle differenti unità organizzative coinvolte, la Società si è dotata di uno specifico processo di *compliance,* di seguito rappresentato in forma grafica, articolato in diverse attività il cui svolgimento viene considerato idoneo a garantire l'adeguato presidio degli ambiti normativi individuati.

A supporto delle diverse attività di compliance, la Funzione si è dotata di applicativo GRC (Governance-Risk Management-Compliance), il cui perimetro di adozione ricomprende anche le società italiane del Gruppo Bancario, in fase di progressiva implementazione e consolidamento.

Di seguito si riporta il dettaglio delle singole fasi in cui si articola il processo di *compliance*:

- ***FASE 1: FRAMEWORK***

5.3.1 DEFINIZIONE E VALUTAZIONE PERIODICA DEL FRAMEWORK

L'attività consiste nella definizione delle metodologie per la valutazione del rischio di non conformità e nella individuazione delle relative procedure, al fine di minimizzare le conseguenze sia sanzionatorie sia reputazionali derivanti dalla non corretta applicazione della normativa.

L'attività prevede inoltre una valutazione periodica del *framework* alla luce dell'evoluzione del contesto interno ed esterno di riferimento, proponendo agli Organi aziendali, se del caso, gli interventi da effettuare e gli aggiornamenti da apportare al modello.

- ***FASE 2: PLANNING***

5.3.2 SCOPING NORMATIVO

L'attività di *scoping* normativo consiste nella definizione e nel successivo monitoraggio del quadro normativo rilevante per la Banca.

La finalità dello *scoping* è di identificare il perimetro degli ambiti normativi rilevanti per la Banca, che vengono elencati nella c.d. *Rule Map*. Qualora una norma abbia i requisiti per impattare sul *business* della Banca in termini di rischio di non conformità (considerato in relazione, ad esempio, alla dimensione, complessità e trasversalità dei processi aziendali impattati ed ai prodotti offerti), essa viene inclusa nel perimetro normativo di riferimento.

L'attività di *scoping* è preliminare alle altre attività ricomprese nel processo di Compliance, viene svolta su base annuale in fase di pianificazione delle attività della Funzione previste per il nuovo esercizio e deve tenere conto degli aggiornamenti che intervengono nel periodo.

Al netto delle aree normative escluse dal perimetro di competenza di Compliance (quali, ad esempio Antiriciclaggio e Privacy), una volta identificati gli ambiti normativi da includere secondo un'ottica *risk based*, gli stessi vengono classificati come segue:

- **perimetro diretto**: vengono comprese le normative rilevanti per la Banca e/o quelle fatte ricadere espressamente in tale perimetro dalle normative vigenti e pertanto presidiate in modo diretto ed accentrato a cura della Funzione Compliance[4];
- **perimetro indiretto**: vengono comprese le normative per cui, limitatamente a quanto espresso dalla legge, si può far riferimento ad una funzione tecnico-specialistica in grado di presidiarle.

Al fine di valutare se adottare, su uno specifico ambito normativo, un approccio diretto o indiretto, viene valutata la presenza di funzioni aziendali specialistiche, il livello di focalizzazione delle stesse in ambito normativo, il grado di specializzazione ed il livello di segregazione in termini di generazione del rischio che deve essere monitorato. Si tiene altresì conto della valutazione delle attività svolte l'anno precedente dalle Unità Specialistiche (ove preesistenti). L'autonomia delle Unità Specialistiche avrà differenti gradi a seconda delle caratteristiche specifiche dell'unità stessa.

[4] Si precisa che nell'ambito delle normative rientranti nel perimetro diretto, la Funzione Compliance presidia in particolare i rischi di non conformità correlati ad ambiti che impattano trasversalmente i processi aziendali, quali gli ambiti ICT e le tematiche ESG (*Environmental, Social e Governance*), incluso il cambiamento climatico (*Climate Change*) nell'ambito dei processi che impattano, in modo specifico, sugli aspetti inerenti alla tutela dei clienti attuali e potenziali. Inoltre, la Funzione è tenuta a presidiare e monitorare nel continuo le tematiche inerenti alla gestione delle Operazioni Personali e alla identificazione delle Operazioni Sospette ai fini Market Abuse.

5.3.3 PIANIFICAZIONE ATTIVITÀ DI COMPLIANCE

L'attività di pianificazione della Funzione Compliance, su base triennale, prevede un aggiornamento ed una validazione annuale attraverso la predisposizione di un programma di attività (*Compliance Plan*), da sottoporre agli Organi aziendali, in cui sono identificati i processi aziendali che espongono la Società ai principali rischi e, sui quali, sono programmati i relativi interventi di verifica, tenendo conto sia delle eventuali carenze emerse nei controlli precedentemente svolti, sia di eventuali nuovi rischi identificati a seguito dell'evolversi della normativa e del business della società. Il modello di controllo per processo consente infatti di valutare l'esposizione al rischio di ogni attività che lo compone, valutando i presidi in essere ed eseguendo controlli per determinare la loro efficacia e completezza al fine di esprimere un giudizio sulla conformità del processo stesso alla normativa vigente. Qualora si rilevi un giudizio di mancata conformità, vengono indicati piani di intervento atti a contenere o rimuovere gli eventuali gap riscontrati.

In fase di pianificazione, si tiene conto sia di valutazioni qualitative, correlate alla rilevanza dei processi e delle norme in funzione del *business* esercitato, sia di valutazioni quantitative.

Per quanto concerne le valutazioni qualitative, queste sono ascrivibili principalmente alla necessità di sviluppare l'attività di *compliance* all'interno di quegli ambiti normativi che risultano rilevanti ai fini della tutela del risparmiatore, prestando particolare rilevanza anche agli aspetti che comportano un rischio reputazionale per il Gruppo, nonché avendo in ogni caso un approccio *forward looking* al fine di considerare, laddove possibile, gli aggiornamenti normativi in corso e prospettici.

Per quanto concerne, invece, le valutazioni basate su parametri quantitativi, sono valutati i processi a cui sono associati i rischi di non conformità più rilevanti in funzione delle sanzioni previste.

La metodologia adottata per l'individuazione della rischiosità dei processi (c.d. "rischio inerente") tiene conto non solo del profilo sanzionatorio espresso dalla normativa, ma anche di ulteriori elementi (c.d. *driver*), quali l'incidenza degli eventi di perdita generatisi nell'ambito dei processi aziendali negli esercizi precedenti, gli orientamenti dell'Autorità di Vigilanza e della giurisprudenza, l'analisi dei rilievi emessi dalla Funzione Internal Audit, la presenza di eventuali azioni di mitigazioni in corso, la presenza di perdite operative, gli esiti di precedenti verifiche nonché gli esiti delle analisi svolte dalla Funzione Risk Management (c.d. *Risk Factors Control Assessment* -RFCA).

Anche le evidenze emerse dall'analisi periodica dei Key Compliance Indicators (KCI) sono di supporto per indirizzare la pianificazione dei controlli della Funzione (come anche per valutare, in corso d'anno, la necessità di compiere approfondimenti mirati).

La pianificazione delle attività di controllo viene svolta su base triennale, con l'obiettivo di coprire il perimetro normativo di competenza della Funzione, focalizzandosi sui processi maggiormente impattati dal rischio di non conformità. La puntuale pianificazione annuale deve tenere conto, anno per anno, delle eventuali modifiche ed integrazioni che si rendono necessarie sulla base dell'evoluzione della normativa e/o del business.

La pianificazione annuale delle complessive attività della Funzione viene svolta entro il primo trimestre di ciascun esercizio e portata all'attenzione del Comitato Rischi nonché del Consiglio di Amministrazione per la relativa approvazione.

- ***FASE 3: ADVISORY & BUSINESS IMPACT***

5.3.4 CONSULENZA E FORMAZIONE

L'attività consiste nel fornire:

- "Consulenza", finalizzata a prestare assistenza agli Organi Aziendali ed alle funzioni interessate, in tutte le materie in cui il rischio di non conformità assume particolare rilievo, ivi compresa l'operatività in nuovi prodotti e servizi e la coerenza del sistema premiante aziendale.
- "Collaborazione" con le strutture preposte nell'attività di formazione del personale e della rete di vendita per le tematiche in cui assumono rilevanza significativa gli aspetti di compliance, al fine di diffondere una cultura aziendale improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme.
- "Validazione" di documenti, testi, materiale info-formativo e pubblicitario, contrattualistica predisposti da specifiche funzioni aziendali, per quanto concerne gli aspetti attinenti al rischio di non conformità.

5.3.5 MONITORAGGIO EVOLUZIONI NORMATIVE E ALERT

L'attività consiste nell'effettuare un monitoraggio costante dell'evoluzione del contesto normativo di riferimento per fornire indicazioni sintetiche alle strutture interessate circa le nuove normative rilevanti (a*lert* normativo). L'obiettivo è quello di rilevare tempestivamente ed efficacemente innovazioni e gli aggiornamenti legati a:

- disposizioni legislative e regolamentari, ancorché in consultazione;
- indicazioni delle associazioni di categoria;
- orientamenti giurisprudenziali.

Tale attività di monitoraggio è svolta sia tramite consultazione diretta delle fonti normative che su input e con il supporto di soggetti esterni.

Se sono intervenute modifiche nel perimetro normativo di riferimento tali da impattare sul *business* della Banca, ne viene data pronta comunicazione alle unità organizzative coinvolte.

5.3.6 ANALISI DI IMPATTO E VALUTAZIONE DI ADEGUATEZZA EX ANTE

La Funzione Compliance, a seguito dell'invio dell'alert, laddove in considerazione delle novità normative intervenute sia ritenuto necessario procedere con un'analisi di dettaglio:

- effettua l'analisi di dettaglio delle novità normative ed identifica gli adempimenti normativi richiesti, rispetto al modello operativo specifico della Banca;
- identifica i gap normativi e i rischi di non conformità derivanti dall'introduzione dei nuovi adempimenti normativi e trasmette la gap analysis alle strutture organizzative impattate, coinvolgendo se opportuno anche la Divisione Organizzazione e Project Management per un eventuale supporto nell'identificazione della struttura di coordinamento progettuale;
- fornisce il supporto necessario agli owner preposti per identificare gli adeguamenti e i presidi necessari per colmare i gap normativi identificati ed assicurare un adeguato presidio dei rischi di non conformità individuati, richiedendo agli owner di allineare la Funzione rispetto alla fase di implementazione delle

soluzioni individuate, con particolare riferimento ad eventuali necessità di revisione delle stesse sia in termini di contenuto sia di tempistiche per il rilascio.

La necessità di adeguamento può inoltre essere originata da progetti innovativi che potrebbero modificare l'assetto organizzativo o procedurale (inclusa l'operatività in nuovi prodotti o servizi) della Banca. È pertanto previsto il coinvolgimento della Funzione Compliance nella valutazione *ex ante* della conformità alla regolamentazione applicabile di tutti i progetti innovativi che la Banca intenda intraprendere.

A tal fine, la Funzione Compliance fornisce consulenza specialistica su progetti innovativi in cui può essere presente un rischio di non conformità e ne valuta *ex ante*, su richiesta della funzione aziendale proponente, la conformità alla regolamentazione applicabile con riferimento, in particolare, alla commercializzazione di nuovi prodotti e servizi (o alla modifiche sostanziali apportate ai prodotti, processi e sistemi esistenti) e alla modifica del sistema premiante aziendale.

Nell'ambito dell'attività di adeguamento riveniente sia da nuove normative sia da progetti innovativi, la Funzione Compliance svolge pertanto le c.d. verifiche di adeguatezza ex ante attraverso l'identificazione di proposte di modifiche, anche organizzative e procedurali, derivanti anche da *gap analysis*, valutazioni e pareri, al fine di accertare che l'impianto sia conforme alla normativa e, se del caso, formalizzare piani di azione con le strutture aziendali interessate, curandone il successivo follow up prima dell'entrata in vigore della norma o dell'avvio della nuova attività/business.

Nell'ambito delle predette verifiche di adeguatezza "*ex ante*" rientra anche la validazione delle *policy* e di altri documenti di normativa interna (regolamenti, procedure) afferenti alle aree normative rientranti nel perimetro normativo di competenza, in seguito, a titolo esemplificativo, ad eventuali novità normative esterne o a modifiche alla struttura di *governance* ed organizzativa, in linea con quanto previsto dalla "Policy di Conglomerato sulle modalità di redazione, aggiornamento, approvazione e diffusione della Normativa Interna".

Infine, la Funzione Compliance collabora nell'attività di predisposizione delle attività formative per le tematiche in cui assumono rilevanza significativa gli aspetti di compliance.

Con riferimento alle attività di advisory descritte nei precedenti paragrafi, si precisa che le attività svolte dalla Funzione Compliance sono di volta in volta registrate nell'applicativo gestionale della Funzione citato in precedenza, a cura dell'Advisor dell'Unità Advisory e Business Impact che ha prestato il servizio.

- ***FASE 4: CONTROLS***

5.3.7 CONTROLLI EX POST: VERIFICHE DI ADEGUATEZZA E DI FUNZIONAMENTO

I controlli "*ex post"* sono fondati sulla valutazione dello stato di conformità dei processi aziendali rispetto alle norme con l'obiettivo di identificare eventuali violazioni, di valutare la completezza ed adeguatezza dei presidi a fronte di specifici rischi e di proporre gli interventi correttivi atti a superare le eventuali carenze rilevate.
A tal fine la valutazione dei presidi prevede:

- l'analisi del disegno del processo e la valutazione della sua conformità alla normativa vigente;
- l'analisi di procedure interne operative e di controllo atte a mitigare i rischi rilevati;

- la verifica che le stesse siano complete, adeguate, conosciute, efficaci ed attuate con continuità;
- la verifica dell'esistenza di competenze e comportamenti adeguati da parte del personale incaricato dello svolgimento delle attività;
- la verifica dell'affidabilità degli applicativi informatici in termini di adeguatezza di controlli e attendibilità dei dati elaborati o prodotti.

A seguito delle valutazioni sopra descritte possono essere proposte eventuali azioni di mitigazione e interventi correttivi atti a superare le carenze rilevate, che possono prevedere:

- un adeguamento della normativa interna;
- l'attivazione di nuovi presidi e/o controlli;
- l'integrazione di procedure e controlli ICT a supporto di specifiche fasi del processo;
- iniziative di formazione del personale e della Rete di Vendita;
- il rafforzamento dei controlli di linea (c.d. “controlli di I livello”).

Il modello di controllo adottato è articolato nelle seguenti fasi:

- identificazione dei processi e pianificazione delle verifiche;
- esecuzione;
- misurazione della rischiosità rilevata;
- reporting;
- azioni di mitigazione.

5.3.7.1 IDENTIFICAZIONE E PIANIFICAZIONE

L’individuazione dei processi aziendali oggetto di verifica, selezionati con un approccio *risk-based* e in funzione della loro rilevanza rispetto al modello di business della Banca, e la relativa pianificazione delle attività sono effettuati in coerenza con il perimetro normativo assunto (*Rule Map)*. In questa prima fase, in particolare, il rischio di non conformità (*compliance risk*) è ricondotto al processo, come da alberatura dei processi aziendali, a cui viene associato un *risk impact* (ovvero rischio inerente, che può assumere i seguenti valori: Alto, Medio Alto, Medio Basso, Basso) e, come già anticipato nel par. 5.3.3, tiene in considerazione, oltre alla tipologia di sanzione a cui la società potrebbe essere esposta, anche ulteriori *driver*, quali l’incidenza degli eventi di perdita generatisi nell’ambito dei processi aziendali negli esercizi precedenti, gli orientamenti dell’Autorità di Vigilanza e della giurisprudenza, l’analisi dei rilievi emessi dalla Funzione Internal Audit, la presenza di eventuali azioni di mitigazioni in corso, la presenza di perdite operative, gli esiti di precedenti verifiche nonché gli esiti delle analisi svolte dalla Funzione Risk Management (c.d. *Risk Factors Control Assessment* -RFCA).

A supporto della pianificazione dei controlli, vengono inoltre considerate le evidenze scaturite dall’analisi e dal monitoraggio periodico dei Key Compliance Indicators (KCI), quali indicatori di possibili aree di attenzione o malfunzionamento.

5.3.7.2 ESECUZIONE

Ogni processo oggetto di verifica viene sottoposto a ricognizione per valutare il suo allineamento ai requirement normativi di riferimento per ciò che attiene all'adeguatezza dell'impianto, al corretto disegno dei presidi e al loro effettivo funzionamento. L'attività di verifica viene svolta tramite:

- interviste con il/i Responsabile/i delle unità aziendali interessate;
- analisi di dettaglio del processo/attività;
- verifiche dirette su base campionaria tramite estrazioni informatiche o analisi documentale.

Le conseguenti valutazioni, per ogni *compliance risk* di riferimento, si fondano sull'analisi delle seguenti tre principali dimensioni:

- *process:* il corretto disegno del processo, la corretta collocazione dei relativi presidi, l'accurata descrizione degli stessi e dei relativi controlli di funzionamento nella normativa interna di riferimento;
- *system*: l'analisi delle procedure di carattere informatico o manuale che supportano lo svolgimento del processo ed i relativi controlli di linea;
- *people*: l'insieme delle attività di formazione del personale addetto allo svolgimento delle attività inerenti al processo in analisi.

Ad ognuna delle tre dimensioni sopra descritte e in riferimento a ciascun *compliance risk*, tramite una scala valutativa, o *score*, viene assegnato un giudizio utilizzando una matrice a quattro livelli, sia per le valutazioni di adeguatezza che di efficacia.

Nella valutazione complessiva del sistema dei presidi sono assegnati "pesi" diversi ad ognuna delle dimensioni d'analisi.

Di seguito si riporta la tassonomia di dettaglio per le valutazioni di adeguatezza e di efficacia.

VALUTAZIONE DI ADEGUATEZZA		
1	Inadeguato	Mancata formalizzazione delle attività del processo oggetto di analisi
2	Parzialmente inadeguato	Le attività a presidio del processo oggetto di analisi risultano essere parzialmente formalizzate in termini di ruoli e responsabilità, tipologia, frequenza e strumenti anche informatici, organicità della normativa interna / ritardi nell'aggiornamento della normativa interna rispetto ad evoluzioni normative
3	Parzialmente adeguato	Le attività a presidio del processo oggetto di analisi risultano essere formalizzate, tuttavia risultano essere presenti margini di miglioramento circa la definizione degli elementi del processo in termini di tipologia, frequenza e strumenti anche informatici, organicità della normativa interna/aggiornamenti formali
4	Adeguato	Gli elementi a presidio del processo oggetto di analisi risultano essere formalizzati in termini di ruoli e responsabilità, tipologia, frequenza e strumenti anche informatici

VALUTAZIONE DI EFFICACIA		
1	Inefficace	Il processo e le attività testate, posti a presidio degli elementi di rischiosità, non risultano eseguiti
2	Parzialmente inefficace	Il processo è svolto in maniera per lo più inefficace rispetto a quanto previsto dalla normativa interna ed esterna e/o rispetto al campione osservato
3	Parzialmente efficace	Il processo è svolto in maniera per lo più efficace rispetto a quanto previsto dalla normativa interna ed esterna e/o rispetto al campione osservato
4	Efficace	Il processo e le attività testate, posti a presidio degli elementi di rischiosità, risultano eseguiti e sono conformi rispetto a quanto previsto dalla normativa interna ed esterna e rispetto al campione osservato

Per completezza si evidenzia inoltre che alcune tematiche, quali ad esempio la gestione delle operazioni su strumenti finanziari effettuate dal personale della Banca o le operazioni di Corporate Finance e Capital Market

poste in essere dalla Direzione Investment Banking, sono presidiate dalla Funzione Compliance anche mediante un presidio continuativo di controllo, volto a garantire maggiore tempestività di verifica rispetto alla sola effettuazione dei controlli ex post definiti nell'ambito della pianificazione annuale.

Ulteriore elemento a supporto delle attività di verifica è rappresentato dall'utilizzo dei cosiddetti *Key Compliance Indicators* (KCI), quali indicatori di possibili aree di attenzione o malfunzionamento sulle quali apportare potenziali interventi di miglioramento dei processi in esame.

5.3.7.3 MISURAZIONE DELLA RISCHIOSITÀ RILEVATA

La valutazione complessiva ed integrata del sistema dei presidi per processo, in termini di adeguatezza ed efficacia, è ottenuta sulla base della valutazione dei singoli *compliance risk* assegnata nella fase di esecuzione dei controlli per ognuna delle tre dimensioni di analisi (*process, system, people*) mediante una ponderazione che consente ai risultati delle verifiche di funzionamento di influire maggiormente sul risultato.

In particolare, la valutazione complessiva dei presidi è espressa tramite una scala valutativa, o *score*, a quattro livelli, in ordine decrescente di severità del giudizio:

- Presidi non soddisfacenti
- Presidi in prevalenza non soddisfacenti
- Presidi in prevalenza soddisfacenti
- Presidi soddisfacenti

secondo la tabella di riconduzione riportata di seguito:

ADEGUATEZZA	VALUTAZIONE COMPLESSIVA PRESIDI			
INADEGUATO	Presidi non soddisfacenti	Presidi non soddisfacenti	Presidi in prevalenza non soddisfacenti	Presidi in prevalenza soddisfacenti
PARZIALMENTE INADEGUATO	Presidi non soddisfacenti	Presidi in prevalenza non soddisfacenti	Presidi in prevalenza soddisfacenti	Presidi in prevalenza soddisfacenti
PARZIALMENTE ADEGUATO	Presidi in prevalenza non soddisfacenti	Presidi in prevalenza non soddisfacenti	Presidi in prevalenza soddisfacenti	Presidi soddisfacenti
ADEGUATO	Presidi in prevalenza non soddisfacenti	Presidi in prevalenza soddisfacenti	Presidi soddisfacenti	Presidi soddisfacenti
	INEFFICACE	PARZIALMENTE INEFFICACE	PARZIALMENTE EFFICACE	EFFICACE
	EFFICACIA			

5.3.7.4 VALORIZZAZIONE DEL RISCHIO RESIDUO PER PROCESSO

Ottenuta la valutazione complessiva del sistema dei presidi, si procede al calcolo del rischio residuo "per processo" mediante "abbattimento" del relativo rischio inerente come riportato nella tabella seguente:

RISCHIO INERENTE	RISCHIO RESIDUO			
ALTO	Sfavorevole: Rischio Alto	Sfavorevole: Rischio Alto	Parzialmente favorevole: Rischio Medio/Basso	Parzialmente favorevole: Rischio Medio/Basso
MEDIO ALTO	Sfavorevole: Rischio Alto	Parzialmente sfavorevole: Rischio Medio/Alto	Parzialmente favorevole: Rischio Medio/Basso	Favorevole: Rischio Basso
MEDIO BASSO	Parzialmente favorevole: Rischio Medio/Basso	Parzialmente favorevole: Rischio Medio/Basso	Parzialmente favorevole: Rischio Medio/Basso	Favorevole: Rischio Basso
BASSO	Favorevole: Rischio Basso	Favorevole: Rischio Basso	Favorevole: Rischio Basso	Favorevole: Rischio Basso
	PRESIDI NON SODDISFACENTI	**PRESIDI IN PREVALENZA NON SODDISFACENTI**	**PRESIDI IN PREVALENZA SODDISFACENTI**	**PRESIDI SODDISFACENTI**
	VALUTAZIONE COMPLESSIVA PRESIDI			

Il rischio residuo associato al singolo processo può quindi assumere i seguenti valori alternativi, in ordine decrescente di severità di giudizio:

- Sfavorevole: Rischio Alto
- Parzialmente sfavorevole: Rischio Medio/ Alto
- Parzialmente favorevole: Rischio Medio/ Basso
- Favorevole: Rischio Basso

Il valore del rischio residuo ottenuto dalle matrici sopra riportate può essere rivisto, in un'ottica prudenziale, dal Compliance Officer in funzione di alcuni elementi quali l'impatto del processo sul modello di business della Società oppure indicazioni/interventi delle Autorità Vigilanza.

Con riferimento alle attività di controllo descritte nei precedenti paragrafi, si precisa che le attività di verifica svolte dalla Funzione Compliance sono supportate dall'applicativo gestionale della Funzione citato in precedenza e vengono registrate nello stesso a cura dell'Analista dell'Unità Controls responsabile del singolo intervento.

5.3.7.5 AZIONI DI MITIGAZIONE

A fronte del completamento delle analisi di adeguatezza e di funzionamento, ove sia riscontrato un gap rispetto a quanto normativamente richiesto, la Funzione identifica le opportune azioni di mitigazione, assegnando un livello di priorità riconducibile al rischio sotteso al singolo gap.

Il livello di priorità associato alla azione di mitigazione in fase di emissione della stessa può assumere i seguenti valori alternativi:

- Alto
- Medio Alto
- Medio Basso
- Basso

Le azioni di mitigazione vengono condivise con i responsabili delle strutture aziendali interessate (c.d. *owner*), avvalendosi, ove necessario, del supporto della Divisione Organizzazione e Project Management e/o della Divisione ICT. Le azioni di mitigazione sono registrate nell'applicativo gestionale della Funzione, con indicazione della tempistica prevista per la loro attuazione e sono oggetto di regolare monitoraggio, interagendo, ove necessario, con l'owner dell'azione e con le unità organizzative responsabili degli interventi di adeguamento.

Le azioni di mitigazione ed il relativo stato di avanzamento sono inoltre oggetto di rendicontazione periodica agli Organi Aziendali.

In tale ambito, Banca Mediolanum si è dotata del *Regolamento del processo di gestione dei rilievi emessi dalle Funzioni Aziendali di Controllo* con l'obiettivo di:

- descrivere le diverse fasi del processo che le competenti strutture aziendali devono porre in essere per la gestione ed il monitoraggio dei rilievi emessi dalla Funzioni Aziendali di Controllo;
- identificare ruoli, compiti e responsabilità degli attori coinvolti;
- rafforzare l'adozione progressiva di metodologie e prassi operative uniformi tra le Funzioni Aziendali di Controllo.

Il predetto Regolamento ha previsto inoltre una maggiore declinazione delle tipologie di azioni di mitigazione: in particolare, sono stati introdotti i nuovi concetti di:

- Azione "di *contingency*": soluzione a carattere temporaneo che consenta di mitigare i rischi rilevati in attesa della conclusione delle azioni identificate (tale intervento si rende necessario con particolare riferimento ai "punti di adeguamento" classificati con priorità "Alta");
- Azione "di *design*": intervento di progettazione e stima in termini di tempi e costi della successiva azione di natura implementativa, in caso di rilievi complessi, su iniziativa dell'unità organizzativa responsabile dell'intervento di adeguamento, in accordo con la Funzione di Controllo e da concludersi in ogni caso entro un tempo massimo di sei mesi.

5.3.7.6 REPORTING DELLE ATTIVITA' DI VERIFICA

L'attività di verifica viene conclusa con la formalizzazione di appositi report, condivisi con i Responsabili delle unità organizzative sottoposte ad analisi, nei quali vengono descritti almeno i seguenti aspetti:

- la sintesi degli esiti della verifica (c.d. Executive Summary), con l'immediata evidenza delle eventuali azioni di mitigazione proposte;

- l'obiettivo e il perimetro delle attività di controllo;
- il quadro normativo di riferimento;
- l'identificazione delle unità organizzative coinvolte;
- gli applicativi informatici coinvolti;
- le verifiche effettuate, sia di adeguatezza che di funzionamento;
- i risultati dell'intervento;
- gli esiti di eventuali "*follow up*" effettuati su verifiche precedenti.

5.3.8 ANALISI INDICATORI DI RISCHIO (KCI)

La prevenzione dei rischi di non conformità è legata anche alla tempestiva rilevazione di segnali sintomatici di situazioni rischiose, che potrebbero comportare un danno diretto o indiretto di natura sanzionatoria, economica o reputazionale.

Nell'ambito del complessivo framework di controllo e mitigazione dei rischi, la Funzione Compliance si avvale anche di apposito cruscotto (*risk dashboard*) per l'analisi ed il monitoraggio a distanza dei comportamenti operativi riguardo a taluni ambiti normativi. A tal proposito, provvede mensilmente alla raccolta, all'elaborazione e all'analisi di dati relativi a fattori di rischio di non conformità, i *Key Compliance Indicators* (KCI). Gli indicatori raccolti non sono necessariamente fonte di un rischio di non conformità, ma sono elementi che, a seguito di opportuni approfondimenti, potrebbero mettere in luce eventuali anomalie, errori o malfunzionamenti, ovvero *trend* di business che possano comportare la necessità di definire ulteriori presidi di mitigazione del rischio di compliance.

Le evidenze risultanti dall'analisi periodica dei KCI sono inoltre di supporto per indirizzare l'attività di controllo ex post della Funzione ovvero per valutare, in corso d'anno, la necessità di compiere specifici approfondimenti.

A livello metodologico, gli indicatori sono distinti in tre categorie:

- *Esposizione*: indicatori dimensionali che monitorano l'andamento di grandezze patrimoniali, economiche ed organizzative rilevanti per l'azienda, a supporto della comprensione, anche operativa, dei processi che rappresentano;
- *Allerta*: indicatori dimensionali il cui andamento anomalo, sulla base di soglie predefinite, può essere segnale di eventi di non conformità, che sono già in essere o per i quali vi è una forte probabilità di accadimento;
- *Anomalia*: indicatori di tipo "*on/off*", che misurano la presenza di un rischio di non conformità.

Con specifico riferimento agli indicatori di Allerta, questi sono suddivisi in quattro classi di rischio dalle quali può dipendere l'attivazione di apposite procedure finalizzate al monitoraggio analisi del fenomeno evidenziato dall'indicatore medesimo. Di seguito si dettagliano le predette classi di rischio, unitamente alle rispettive procedure previste:

Basso	Nessuna attivazione.
Medio Basso	Monitoraggio andamentale da parte dell'unità Framework, Reporting e Coordinamento di Gruppo (FR&CG).
Medio Alto	Attivazione analisi di dettaglio da parte dell'unità FR&CG e, nel caso di necessità di eventuali azioni correttive, coinvolgimento della unità Advisory & Controls.
Alto	Attivazione analisi di dettaglio da parte dell'unità FR&CG ed informativa alle unità Advisory & Controls, che forniscono ausilio nella mappatura di eventuali azioni correttive. Sulla base delle criticità emerse dalle analisi svolte è previsto un coinvolgimento immediato del Compliance Officer di Gruppo.

Sono inoltre stati definiti alcuni "indicatori sintetici", che integrano le misurazioni dei singoli indicatori, al fine di consentire la valutazione complessiva dei risultati emersi da gruppi di KCI omogenei per ambito normativo, per rilevare ed osservare eventuali fenomenologie complessive.

Ai fini dell'applicazione del modello, i singoli indicatori sono stati calcolati sullo stesso intervallo temporale e possono assumere un valore ricompreso tra 0 e 100, crescente in relazione al livello di diffusione del fenomeno analizzato.

Gli indicatori di allerta prevedono delle soglie che rappresentano il limite oltre il quale la situazione osservata richiede specifiche analisi ed approfondimenti con le unità organizzative interessate, a seguito dei quali può scaturire una specifica azione di mitigazione.

Gli esiti risultanti dalla applicazione delle regole sopra esplicitate possono essere prudenzialmente rivisti dal Compliance Officer secondo valutazioni che tengano conto di alcuni elementi, quali l'emanazione di nuove normative o l'evoluzione del *business* della Società.

- ***FASE 5: REPORTING***

5.3.9 REPORTING AGLI ORGANI AZIENDALI E ALLE AUTORITÀ DI VIGILANZA

5.3.9.1 REPORTING AGLI ORGANI AZIENDALI

La Funzione Compliance, con cadenza almeno annuale, presenta agli Organi aziendali una relazione dell'attività svolta, che illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati e propone gli interventi da adottare per la loro rimozione. In ogni caso, informa tempestivamente gli Organi aziendali su ogni violazione o carenza rilevante riscontrate (ad esempio, violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo, o significativi impatti sulla situazione finanziaria o patrimoniale, danni di reputazione, malfunzionamenti di procedure informatiche critiche).

Inoltre, con cadenza trimestrale, sottopone al Comitato Rischi ed al Consiglio di Amministrazione una relazione periodica sull'attività svolta, sia con riferimento alle attività di advisory che alle attività di controllo, da inoltrare altresì, ove richiesto, alle Autorità di Vigilanza.

5.3.9.2 REPORTING AD AUTORITÀ DI VIGILANZA

La Funzione Compliance cura la predisposizione delle relazioni periodiche alle Autorità di Vigilanza in ottemperanza agli obblighi normativi nonché secondo le tempistiche e le modalità definite.

Nell'ambito, infine, dei rapporti con le Autorità di Vigilanza nazionali, compete alla Funzione Compliance il presidio delle relazioni con queste ultime e con le Associazioni di Categoria, per le tematiche di diretta competenza.

Rientra in tale ambito il presidio della corretta gestione delle istanze provenienti dalle Autorità di Vigilanza nazionali, nonché la partecipazione a gruppi di lavoro associativi per tematiche specialistiche di competenza.

Con particolare riferimento al presidio delle comunicazioni/istanze trasmesse alla Banca e alle altre società italiane del Gruppo Bancario dalle diverse Autorità di Vigilanza nazionali, la Funzione Compliance cura:

- la registrazione delle istanze ricevute e l'indirizzamento agli Uffici pertinenti per la relativa evasione, monitorando il rispetto dei tempi previsti per la trasmissione dell'eventuale risposta;
- l'analisi delle decisioni dell'Arbitro Bancario Finanziario e dell'Arbitro per le Controversie Finanziarie, svolta avvalendosi di specifici flussi posti in essere con la Direzione Affari Societari, Legali e Contenzioso, finalizzata a verificare la conformità dei processi e delle procedure aziendali e ad assicurare che le preposte funzioni ne tengano in debito conto nella gestione dei reclami della clientela;
- l'integrazione delle informazioni specialistiche sull'interpretazione ed applicazione delle norme sulla scorta delle evidenze delle istanze e dei contatti con le Autorità di Vigilanza.

Inoltre, riceve le richieste inviate dalle controparti istituzionali ai referenti contrattuali e/o operativi e coordina le diverse unità organizzative interessate al fine di garantirne adeguata evasione e archiviazione.

5.4 Modello di Coordinamento tra le Strutture Coinvolte nel Presidio del Rischio di Non Conformità

5.4.1 Linee guida di coordinamento con le Unità Specialistiche

Sulla base dell'adozione di un Modello di Compliance c.d. "graduato", il coordinamento funzionale con le Unità Specialistiche avviene attraverso la redazione dei c.d. "Questionari di Attestazione": essi sono prodotti da ciascuna delle Unità Specialistiche per ogni ambito normativo presidiato. La periodicità di formalizzazione delle Attestazione della Banca è trimestrale.

Le Attestazioni si configurano come un questionario di autovalutazione a compilazione progressiva con una struttura articolata sulla base delle macro aree di attività del processo di Compliance delegate alle Unità Specialistiche relative al monitoraggio delle evoluzioni normative, alla consulenza e alla formazione.

Per ogni fase, le Unità esprimono, in coerenza con la metodologia in uso presso la Funzione Compliance, un giudizio complessivo qualitativo basato sulla seguente scala di valori: Alto, Medio Alto, Medio Basso, Basso.

I giudizi espressi all'interno delle singole attestazioni sono oggetto di analisi da parte della Funzione Compliance e di condivisione con il Responsabile della Unità Specialistica per eventuali approfondimenti necessari in merito alle criticità individuate ed ai relativi piani correttivi predisposti. Sulla base di proprie autonome valutazioni, la Funzione Compliance, a fronte delle Attestazioni ricevute e della rilevanza della normativa in perimetro, può procedere con lo svolgimento di ulteriori attività di controllo e/o di approfondimento su specifiche tematiche.

E' in ogni caso compito delle Unità Specialistiche informare tempestivamente la Funzione Compliance su ogni violazione o carenza rilevante riscontrata (a titolo di esempio, violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o significativi impatti sulla situazione finanziaria o patrimoniale, danni di reputazione, malfunzionamenti di procedure informatiche critiche), nonché sulle novità normative analizzate e sugli interventi di adeguamento avviati.

5.4.2 LINEE GUIDA DI COORDINAMENTO TRA LA FUNZIONE COMPLIANCE E LE ALTRE FUNZIONI DI CONTROLLO

L'interazione tra la Funzione Compliance e le altre Funzioni di Controllo si inserisce, inoltre, nel più generale coordinamento tra tutte le Funzioni ed Organi con compiti di controllo come definito ed espressamente approvato dall'Organo con funzione di supervisione strategica al fine di assicurare il corretto funzionamento del Sistema dei Controlli Interni sulla base di una proficua interazione, evitando sovrapposizioni o lacune. Si rinvia pertanto allo specifico documento "Linee Guida e principi base di coordinamento tra Organi e Funzioni di Controllo", approvato dal Consiglio di Amministrazione della società.

5.4.3 PROTOCOLLI DI COLLABORAZIONE

Le interrelazioni tra la Funzione Compliance e le altre strutture aziendali possono essere formalizzate anche attraversi i c.d. "Protocolli di Collaborazione e coordinamento", documenti predisposti al fine di definire e illustrare le relazioni e gli ambiti di collaborazione reciproca tra le funzioni di controllo e/o le altre strutture aziendali, nonché le rispettive responsabilità nello svolgimento delle attività in ambito, in linea con il documento "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna".

5.4.4 INTERRELAZIONI CON LE ALTRE FUNZIONI COMPLIANCE DEL GRUPPO

La Funzione Compliance di Banca Mediolanum svolge attività di supervisione e coordinamento in relazione alle omologhe funzioni delle società controllate "locali" ed "estere".

A tal fine sono stati identificati e predisposti adeguati flussi informativi da e verso la Capogruppo, periodici o "ad evento", al fine di indirizzare e condividere ogni informazione rilevante per il presidio del rischio di non conformità alle normative in perimetro.

5.4.4.1 FLUSSI INFORMATIVI DALLA FUNZIONE COMPLIANCE DI CAPOGRUPPO VERSO LE FUNZIONI DI COMPLIANCE DELLE SOCIETÀ CONTROLLATE

La Compliance di Capogruppo comunica e condivide con le Funzioni Compliance delle società controllate:

- i contenuti delle Policy di ownership della Funzione oggetto di prossima emanazione, preliminarmente ad ogni aggiornamento delle stesse (ad evento);
- le iniziative progettuali nelle quali è coinvolta e che abbiano impatto sulle Funzioni Compliance delle controllate in termini di processi, strumenti e metodologie in uso (ad evento);

- il piano annuale dei controlli (annualmente) ed eventuali esiti di interesse per le società controllate (ad evento);
- il piano di formazione delle risorse (annualmente).

5.4.4.2 FLUSSI INFORMATIVI DALLA FUNZIONE COMPLIANCE DELLE SOCIETÀ CONTROLLATE ALLA FUNZIONE COMPLIANCE DI CAPOGRUPPO

Le Funzioni Compliance delle società controllate comunicano alla Funzione Compliance di Capogruppo:

- la pianificazione delle attività della Funzione preliminarmente alla approvazione nei rispettivi Organi di Vertice (annualmente) e il relativo stato di avanzamento (almeno trimestralmente);
- l'esito delle verifiche effettuate nonché le azioni di mitigazione identificate ed il relativo avanzamento (almeno trimestralmente);
- le sedute Consiliari di recepimento delle policy di ownership della Funzione (ad evento);
- ogni eventuale evoluzione delle normative locali che impatti in modo significativo sull'andamento business e/o sul perimetro/entità dei rischi di non conformità complessivamente gestiti (ad evento);
- tempestivamente, l'avvio di nuove ispezioni da parte delle Autorità di Vigilanza locali ed ogni interazione intercorsa con le stesse (ad evento);
- il piano di formazione delle risorse (annualmente);
- variazioni significative di assetto organizzativo della Funzione Compliance locale e/o nomine di nuovi responsabili di Funzione o delle eventuali relative unità organizzative di appartenenza.

5.5 INDICATORE SINTETICO DEGLI ESITI DEI CONTROLLI DI COMPLIANCE

Tra i dati e le informazioni che possono essere oggetto di reporting periodico, in particolare verso gli Organi Aziendali e verso le altre Funzioni di Controllo, rientra un indicatore di sintesi degli esiti dei controlli effettuati dalla Funzione Compliance in un determinato periodo di riferimento. La Funzione si è dotata in particolare di un indicatore che sintetizza i risultati delle verifiche di compliance svolte in un periodo di osservazione (tipicamente un anno), andando a considerare il rischio residuo risultante per i singoli *compliance risk* associati ai processi oggetto delle verifiche completate nel periodo in esame.

L'indicatore sintetico complessivo di rischio residuo è il risultato della somma dei singoli indicatori di rischio relativi ai *compliance risk* in perimetro. Viene in prima istanza calcolato in forma percentuale e quindi ricondotto alla scala qualitativa di rischio Alto, Medio Alto, Medio Basso, Basso.

Tale indicatore può essere inoltre integrato nell'ambito della complessiva *dashboard* di indicatori di rischio monitorati nel continuo e rendicontati periodicamente dalla Funzione Risk Management.

6 Normativa esterna di riferimento

I principali riferimenti normativi e regolamentari in tema di gestione del rischio di non conformità utilizzati per la stesura del presente documento sono:

- Circolare n.285 del 17 dicembre 2013 e successivi aggiornamenti;
- D. Lgs. 1° settembre 1993, n° 385 – Testo Unico Bancario – e successivi aggiornamenti;
- Regolamento Consob n. 20307/2018 (Intermediari);
- Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (MiFID II);
- Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (MiFIR). Linee guida ESMA Compliance;
- Decreto legislativo n. 58/1998 (TUF);
- Direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio, del 20 gennaio 2016 sulla distribuzione assicurativa (IDD);
- Decreto Legislativo n. 209 del 2005 e successive modificazioni ed integrazioni (CAP);
- Regolamento IVASS n. 40 del 2 agosto 2018 in materia di distribuzione assicurativa e riassicurativa, come successivamente modificato e integrato;
- Regolamento IVASS n. 45 del 4 agosto 2020 in materia di requisiti di governo e di controllo dei prodotti assicurativi;
- Orientamenti su alcuni aspetti dei requisiti della MiFID relativi alla funzione di controllo alla conformità (ESMA 35-36-1952 del 06/04/2021);
- Attuazione degli Orientamenti dell'EBA in materia di dispositivi di governance e di controllo sui prodotti bancari al dettaglio (*Provvedimento della Banca d'Italia "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti" adottato il 29 luglio 2009, come successivamente modificato);*
- Regolamento europeo 2019/2088 in merito alla "Informativa sulla sostenibilità nel settore dei servizi finanziari" *(Sustainable Finance Disclosure Regulation – SFDR);*
- Regolamento UE n. 852/2020 ("Tassonomia UE").

7 Normativa interna di riferimento

Si richiamano di seguito i principali documenti di normativa interna di Banca Mediolanum, riconducibili alla mission ed al perimetro di azione della Funzione Compliance:

- Ordinamento dei servizi di Banca Mediolanum;
- Progetto di Governo Societario;
- Linee guida e principi base di coordinamento di Gruppo tra Organi e Funzioni di Controllo;
- Policy per la nomina, rimozione e sostituzione dei Responsabili delle Funzioni aziendali di Controllo;
- Regolamento del processo di Indirizzo e Coordinamento del Gruppo Mediolanum;
- Regolamento del processo di gestione dei rilievi emessi dalle Funzioni Aziendali di Controllo.