FLOWE S.p.A. SB

Compliance Policy

Consiglio di Amministrazione del 12 Dicembre 2023

INDICE

1 Premessa

Scopo del presente documento è fornire una descrizione dei principi adottati da Flowe S.p.A. (nel seguito anche “Flowe” o “Flowe S.p.A Società Benefit") in tema di gestione del rischio di non conformità, in linea con il complessivo framework metodologico adottato dalla Capogruppo Banca Mediolanum SpA.

1.1 CONTESTO DI RIFERIMENTO

Il rispetto delle norme rappresenta un elemento fondamentale nello svolgimento dell’attività finanziaria. 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 finanziaria. 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 istituti di dotarsi di articolati Sistemi di Controllo Interno e specifici presidi organizzativi - tra cui 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 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 nuovi prodotti, servizi o modifiche al sistema premiante aziendale che la Società intenda intraprendere.

1.2 OBIETTIVI DEL DOCUMENTO

Flowe S.p.A. Società Benefit (di seguito anche “Flowe” o la “Società”) 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 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. La nostra organizzazione, infatti, prevede un sistema di regole che, indicando principi di carattere generale, integrati da linee guida applicative,

“best practice” 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, pertanto, l’utilizzo di una leva strategica che prevede la possibilità di focalizzarsi, in relazione alla propria dimensione e complessità organizzativa, con maggiore efficacia sulle aree più sensibili e più meritevoli di controllo, modulando le attività di controllo in coerenza al profilo di rischio individuato.

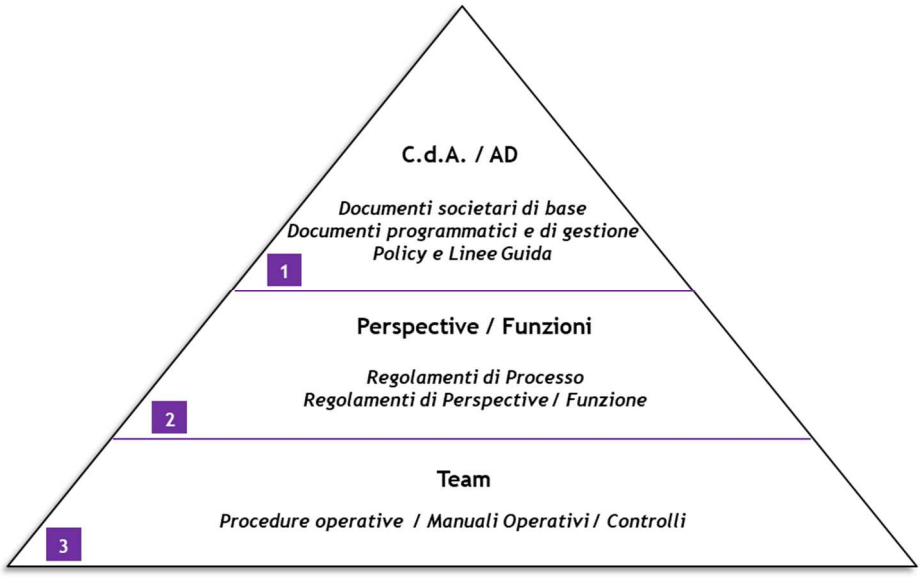
A tal fine, viene emanato il presente documento che fornisce le linee di indirizzo ed identifica i requisiti da rispettare per la definizione del modello di controllo sul rischio di conformità e per la corretta gestione (articolata nelle fasi di progettazione, realizzazione e manutenzione) di un modello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

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

- regole di governo e le politiche di gestione dei rischi di non conformità;
- modalità di gestione del rischio di non conformità in Flowe; :
    - formalizza le modalità di definizione del 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 .

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



2 Applicabilità

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Flowe S.p.A. Società Benefit, nell'ambito dei compiti ad esso affidati dalla normativa di vigilanza sul Sistema dei Controlli Interni. Il suddetto documento è stato ricevuto dalla Capogruppo Banca Mediolanum S.p.A. per l'adozione da parte delle Società facenti parte del Gruppo Banca

rio, secondo un principio di proporzionalità e tenuto conto delle normative e specificità locali, ivi comprese le caratteristiche delle attività di business.

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): Responsabile della Protezione dei Dati ("Data Protection Officer" o "DPO") in conformità al Regolamento Europeo 2016/679 in materia di protezione dei dati personali ("General Data Protection Regulation" o "GDPR"), nominato dal Consiglio di Amministrazione.

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 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. All'interno della Funzione Compliance - parte integrante del Sistema dei Controlli Interni - l' Unità ICT Compliance e Advisory & Controls Flowe ha la responsabilità del presidio dell'evoluzione normativa, dell'analisi degli impatti derivanti dall'applicazione dei nuovi adempimenti, della consulenza specialistica e delle verifiche di adeguatezza e di funzionamento relativamente agli ambiti normativi ICT e sicurezza.

Funzioni di Controllo: le Funzioni Aziendali di Controllo, 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; esso è rappresentato dal Collegio Sindacale.

Organo con funzione di supervisione strategica*:* organo nel quale si concentrano le funzioni di indirizzo e/o di supervisione della gestione sociale (ad esempio, mediante esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche della Società).

Organo con funzione di gestione*:* organo aziendale o componenti di esso ai quali spettano o sono delegati compiti di gestione, ossia l'attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica.

Revisione interna (c.d. "controlli di terzo livello"), l'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: il livello di rischio (complessivo e per tipologia) che la Società intende assumere per il perseguimento dei suoi obiettivi strategici.

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 Organizzativa con competenze specialistiche*:* l'unità organizzativa che presidia taluni ambiti normativi specifici in quanto dotata di competenze e professionalità sui medesimi.

Unità Organizzative: 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 Flowe, la responsabilità dello sviluppo e della gestione della politica di conformità è affidata al Responsabile della Funzione Compliance, nominato da parte dell'organo aziendale competente, che riporta funzionalmente al "**Compliance Officer di Gruppo"** per l'attuazione del modello di *compliance* all'interno della propria realtà aziendale. Al Compliance Officer di Gruppo 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.

Temporanea assenza del Compliance Officer

Per disciplinare le ipotesi In caso di assenza od impedimento del Compliance Officer di Gruppo, la Capogruppo 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..

In caso di assenza temporanea del Compliance Officer delle società controllate e quindi di Flowe, le responsabilità e le attività sono temporaneamente affidate al Compliance Officer di Gruppo.

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 un accordo.

A tale riguardo Flowe, ha esternalizzato lo svolgimento delle attività di compliance alla Funzione Compliance della Capogruppo Banca Mediolanum.

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'attribuzione alle altre **Funzioni Aziendali di Controllo** della responsabilità degli ambiti normativi alle stesse demandati *ex lege,* riferendo direttamente agli Organi Aziendali competenti.

Tale modello prevede inoltre che la Funzione Compliance, per le materie non rientranti nel novero di quelle di propria competenza e in ogni caso, potrà avvalersi della collaborazione e del supporto di talune Unità Organizzative che hanno il compito di assicurare, nel continuo, la conformità delle attività e dei processi alla normativa di rispettiva competenza, disponendo al loro interno di competenze tecniche idonee a supportarla nell'approfondimento di specifiche tematiche. Il supporto potrà avere ad oggetto l'analisi di dettaglio delle novità normative, l'identificazione di rischi e la definizione dei macro interventi.

4.2.1. Funzione Compliance

La Funzione Compliance presiede la gestione dei rischi di non conformità alle norme, secondo un approccio risk based, con riguardo all'attività aziendale e valuta l'adeguatezza delle procedure interne rispetto all'obiettivo di prevenire la violazione di norme imperative (leggi e regolamenti) e di autoregolamentazione (statuti, codici di condotta, codici di autodisciplina) applicabili all'intermediario finanziario. A tal fine:

a. identifica nel continuo le norme applicabili all'intermediario finanziario e alle attività da esso prestate e ne misura/valuta l'impatto sui processi e sulle procedure aziendali;

b. propone modifiche organizzative e procedurali volte ad assicurare l'adeguato presidio dei rischi di non conformità alle norme identificate;

c. predispone flussi informativi diretti agli organi aziendali e alle altre funzioni/strutture aziendali coinvolte;

d. verifica preventivamente e monitora successivamente l'efficacia degli adeguamenti organizzativi suggeriti per la prevenzione del rischio di non conformità.

La funzione di conformità alle norme è coinvolta nella valutazione ex ante della conformità alla regolamentazione applicabile di tutti i progetti innovativi (inclusa l'operatività in nuovi prodotti o servizi) che

l'intermediario intenda intraprendere nonché nella prevenzione e nella gestione dei conflitti di interesse anche con riferimento ai dipendenti e agli esponenti aziendali.

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, con quello di Gestione ed all'Organo con funzione di controllo e comunica con essi senza restrizioni o intermediazioni;
  - deve disporre di un budget autonomo e adeguato per la pianificazione e la gestione dei propri interventi;
- la Funzione Compliance deve essere in una posizione sufficientemente indipendente da poter manifestare il proprio giudizio, esprimere pareri e fornire raccomandazioni in modo imparziale. Essa deve essere scevra 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 è sottoposta. Inoltre, deve essere immune da indebite interferenze che possono limitare o modificare la sua sfera d'azione o lo svolgimento delle sue funzioni, o ancora che possano intaccare o influenzare significativamente il suo giudizio ovvero il contenuto del proprio lavoro. La Funzione non può essere contemporaneamente impiegata in altre attività che potrebbero essere in conflitto con il proprio ruolo.
- Il sistema di remunerazione e incentivazione del Responsabile e del personale della Funzione Compliance deve essere conforme alla regolamentazione di Vigilanza nonché alle politiche interne.

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 Società 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. 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.

4.2.3. 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.

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)".*

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, 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 le normative per le quali la regolamentazione già prevede una stretta competenza della Funzione Compliance come ad esempio per quelle connesse alla trasparenza nei confronti della clientela, agli ambiti ICT e di sicurezza informatica e, più in generale, alla disciplina posta a tutela del consumatore.

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, articolato in diverse attività il cui svolgimento viene considerato idoneo a garantire l'adeguato presidio degli ambiti normativi individuati.

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 adottare e gli aggiornamenti da apportare.

- ***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 Società.

La finalità dello *scoping* è di predisporre un documento, la c.d. *Rule Map*, che ricomprenda tutti gli ambiti normativi rilevanti. Qualora una norma abbia i requisiti per impattare sul *business* della Società in termini di rischio di non conformità (considerato in relazione, ad es., alla dimensione dei processi rilevanti 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 sulla base

della *Rule Map* definita per l'anno precedente e deve tenere conto degli aggiornamenti che intervengono nel periodo.

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. Con riferimento agli ambiti ICT e sicurezza informatica, presidiati dall'Unità ICT Compliance & Controls Flowe, tali *driver* vengono utilizzati considerando elementi specifici relativi agli aspetti ICT (es. presenza di rilievi in audit ICT); in aggiunta, tale Unità considera tra i *driver* anche la presenza di gravi incidenti operativi e di sicurezza, in ragione del perimetro normativo presidiato.

Per quanto concerne, invece, le valutazioni basate su parametri quantitativi, le medesime possono essere supportate da almeno due distinti fattori: da un lato, sono valutati i processi a cui sono associati i rischi di non conformità più rilevanti in funzione delle sanzioni previste, dall'altro, è possibile guidare la pianificazione anche attraverso l'incidenza degli eventi di perdita generatisi nell'ambito di determinati processi aziendali nell'esercizio precedente.

La pianificazione è svolta annualmente entro il primo trimestre di ciascun esercizio e portata all'attenzione del Consiglio di Amministrazione per la relativa approvazione.

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

5.3.4. Consulenza e formazione

L'attività, prestata dalla Unità ICT Compliance e Advisory & Controls Flowe per tutti gli ambiti normativi presidiati, inclusi gli ambiti di ICT e sicurezza , 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 sulle disposizioni applicabili alle attività svolte, 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 (alert normativi). L’obiettivo è quello di rilevare tempestivamente ed efficacemente innovazioni ed aggiornamenti legati a:

- disposizioni legislative e regolamentari, ancorchè in consultazione;
- indicazione 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 Società, 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 Società;
- 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 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 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 rivenire da progetti più rilevanti rispetto al business della società che potrebbero modificare l'assetto organizzativo o procedurale (inclusa l’operatività in nuovi prodotti e servizi ovvero di prodotti e servizi già esistenti ma modificati in modo sostanziale o comunque offerti in un nuovo mercato di riferimento) della Società. È pertanto previsto il coinvolgimento della Funzione Compliance nella

valutazione *ex ante* della conformità alla regolamentazione applicabile di tutti i progetti innovativi che Flowe intenda intraprendere.

A tal fine, la Funzione Compliance fornisce la consulenza specialistica sui 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, all'offerta di nuovi servizi 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, 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. In caso di progetti innovativi con impatti rilevanti in ambito ICT e sicurezza, Unità ICT Compliance e Advisory & Controls Flowe è coinvolta dalla struttura aziendale proponente sin dalle fasi di avvio dell'iniziativa al fine di presidiare i rischi connessi a tali progetti.

Nell'ambito delle predette verifiche di adeguatezza "ex ante" rientra la validazione delle *policy* e della normativa interna (regolamenti) afferente alle aree normative rientranti nel perimetro normativo identificato *(*c. d. *Rule Map)* in conseguenza, a titolo esemplificativo, di eventuali novità normative esterne o di modifiche alla struttura di *governance* ed organizzativa, su richiesta della funzione proponente.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.

- ***FASE 4: CONTROLS***

5.3.7. Controlli ex post: verifiche di adeguatezza e di funzionamento

I controlli ex post, effettuati dall' Unità ICT Compliance e Advisory & Controls Flowe per gli ambiti di ICT e sicurezza informatica presidiati, 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 atte a mitigare i rischirilevati e la verifica che le stesse siano conosciute e 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 e, nell'ambito delle verifiche svolte dall' Unità ICT Compliance e Advisory & Controls Flowe, anche l'aderenza agli standard tecnici e alle best practice per le materie ICT, oltre che l'adeguatezza delle misure di sicurezza previste e il loro efficace funzionamento.

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

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

5.3.8. Identificazione e pianificazione

L'individuazione dei processi aziendali oggetto di verifica e selezionati con un approccio risk-based e in funzione della loro rilevanza rispetto al modello di business della società e la relativa pianificazione annuale delle attività è effettuato in coerenza con il perimetro normativo assunto a riferimento secondo quanto identificato nei documenti *Tool di scoping normativo* e *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* (rischio inerente: serious, high, medium, low) e tiene in considerazione, oltre la tipologia di sanzione a cui la società potrebbe essere esposta, anche altri driver, l'evoluzione della normativa e del business aziendale, gli orientamenti dell'Autorità di Vigilanza e della giurisprudenza, l'analisi dei rilievi dell'Internal Auditing e l'esistenza di eventuali azioni di mitigazioni pregresse. Con riferimento agli ambiti ICT e sicurezza presidiati dall' Unità ICT Compliance e Advisory & Controls Flowe, tali *driver* vengono utilizzati considerando elementi specifici relativi agli aspetti ICT (es. presenza di rilievi in audit ICT); in aggiunta, tale Unità considera tra i *driver* anche la presenza di gravi incidenti operativi e di sicurezza, in ragione del perimetro normativo presidiato.

5.3.9. 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 dimensioni di analisi:

- *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'analisidelle procedure di carattere informatico o manuale che supportano lo svolgimento del processo ed i relativi controlli di linea;
- *people*: il corretto dimensionamento e l'insieme delle attività di formazione del personale addetto allo svolgimento delle attività inerenti il processo in analisi.

Con particolare riferimento alle attività di verifica effettuate dall' Unità ICT Compliance e Advisory & Controls Flowe per il proprio perimetro di competenza, le valutazioni vengono svolte in linea con la metodologia di Compliance e con un focus sulla componente system, al fine di valutare anche l'aderenza agli standard tecnici e alle best practice per le materie ICT, oltre che l'adeguatezza delle misure di sicurezza previste e il loro efficace funzionamento.

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

5.3.10. 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			

5.3.11. 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, variazioni nel corpus normativo, interventi delle Autorità di Vigilanza.

5.3.12. 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*). Le azioni di mitigazione prevedono la definizione di una tempistica per la loro attuazione e sono oggetto di regolare monitoraggio a cura della Funzione, 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, la Capogruppo 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 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.

5.3.13. Reporting delle attività di verifica

L'attività verifica viene conclusa con la formalizzazione di appositi reportcondivisi con i Responsabili delle Unità Organizzativesottoposte ad analisi, nei quali vengono descritti:

- 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.

5.3.14. 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, finanziaria o reputazionale.

Nell'ambito del controllo e mitigazione dei rischi, la Funzione Compliance si avvale, per le verifiche di funzionamento, anche di apposito cruscotto (risk dashboard) per l'analisi ed il monitoraggio a distanza dei comportamenti operativi. A tal proposito, provvede mensilmente all'analisi di dati relativi a fattori di rischio di non conformità, i cosiddetti 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, possono mettere in luce eventuali anomalie, errori o malfunzionamenti su cui un eventuale intervento porterebbe a un miglioramento del processo.

Tali evidenze sono di supporto anche al fine di indirizzare l'attività di controllo ovvero di valutare, in corso d'anno, la necessità di compiere specifici approfondimenti, od avviare apposite azioni di mitigazione dei rischi rilevati.

Si possono identificare tre macro-tipologie di indicatori:

- 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 svolti.

- Allerta: indicatori dimensionali il cui andamento anomalo può essere segnale di eventi di rischiosità operativa o di non conformità, che sono già in essere o per i quali vi è una forte probabilità di accadimento.

- Anomalia: indicatori che misurano la presenza di un rischio di non conformità.

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.

I giudizi risultanti dalle regole sopra esplicitate possono essere prudenzialmente rivisti dal Compliance Officer secondo un giudizio che tiene conto di alcuni elementi quale l'emanazione di nuove normative o variazione nel business della Società.

- ***FASE 5: REPORTING***

5.3.15. Reporting agli Organi Aziendali e alle Autorità di Vigilanza

5.3.15.1. 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 es. 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 semestrale sottopone al Consiglio di Amministrazione una relazione sull'attività svolta.

5.3.15.1.2. 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 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, nonché la partecipazione a gruppi di lavoro associativi per tematiche specialistiche di competenza.

Con particolare riferimento al presidio delle istanze di Vigilanza, la Funzione Compliance cura:

- la registrazione delle istanze ricevute dalle Autorità di Vigilanza e l'indirizzamento agli Uffici pertinenti per la relativa evasione, monitorando il rispetto dei tempi previsti;
- l'analisi delle decisioni dell'Arbitro Bancario Finanziario svolta avvalendosi di specifici flussi posti in essere con la Direzione Affari Societari, Legale e Contenzioso, e finalizzata a verificare la conformità dei processi e delle procedure aziendali e di 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 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.

5.4.2. Interrelazioni con la Funzione Compliance del Gruppo

La Funzione Compliance di Flowe è sottoposta alla supervisione ed al coordinamento di Banca Mediolanum. A tal fine fine sono stati identificati e predisposti adeguati flussi informativi da e verso la Capogruppo, al fine di indirizzare e condividere ogni informazione rilevante per il presidio del rischio di non conformità alle normative in perimetro.

- **Flussi informativi dalla Funzione Compliance di Capogruppo verso la Funzione Compliance di Flowe**

La Compliance di Capogruppo comunica e condivide con la Funzione Compliance di Flowe:

- 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 sulla Compliance della società 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).

- **Flussi informativi dalla Funzione Compliance di Flowe alla Funzione Compliance di Capogruppo**

La Funzionie Compliance di Flowe comunica 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 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 interazionei 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.

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:

- 40° aggiornamento della Circolare n. 285 "Disposizioni di vigilanza per le banche" da parte di Banca d'Italia adattata per le IMEL dalle "Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica";
- Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (Information and Communication Technology, ICT) e di sicurezza (EBA/GL/2019/04) emanati dall'EBA il 28 novembre 2019;
- Disposizioni di Vigilanza per gli Istituti di Pagamento e gli Istituti di Moneta Elettronica - luglio 2019 e successivi aggiornamenti;
- D. Lgs. 1° settembre 1993, n° 385 – Testo Unico Bancario – e successivi aggiornamenti.

7. Normativa interna di riferimento

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

- Policy per la nomina, rimozione e sostituzione dei Responsabili delle Funzioni aziendali di Controllo;
- Regolamento del processo di gestione dei rilievi emessi dalle Funzioni Aziendali di Controllo di Banca Mediolanum S.p.A..